

WEB APPLICATION FIREWALL

# FortiWeb Log Reference

**VERSION 5.4**

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



Tuesday, October 27, 2015

FortiWeb 5.4 Log Reference

1st Edition

# Introduction

This document is a detailed reference of all of your FortiWeb appliance's possible log messages. It is organized primarily by the log type:

- [Event](#)
- [Attack](#)
- [Traffic](#)

To look up the meaning of a specific log message, go to the section that matches its **Type** (`type`) field, then look for the table that matches its **ID** (`log_id`).

This document also explains the general structure of FortiWeb log messages, and the meanings of common fields (see [How to interpret FortiWeb logs on page 5](#)).

## Scope

This document provides administrators information about log messages that can be recorded by a FortiWeb appliance.

This document does **not** cover how to configure logging. It assumes you have already configured it, and need to know how to interpret the log messages. For instructions on how to configure logging, see the [FortiWeb Administration Guide](#) or [FortiWeb CLI Reference](#).

# What's new

The list below contains features new or changed in FortiWeb 5.3 and later.

## FortiWeb 5.4

- **FortiSandbox attack log messages** — Attack log messages report on uploaded files that FortiSandbox has identified as a threat.

For complete information about using a file upload restriction policy to submit uploaded files to FortiSandbox for evaluation, see the *FortiWeb Administration Guide*.

## FortiWeb 5.3

- **Messages related to server policy architecture** — To support the new server policy configuration, some event log messages have been removed or replaced. For example, because you now define physical and domain servers within a server pool configuration only, FortiWeb no longer generates log messages for physical or domain server configuration tasks.

For complete information about the architecture changes, see the *FortiWeb Administration Guide*.

- **Messages for new configuration items** generates event log messages for configuration tasks related to new features, including:
  - Server pool session persistence
  - SNI (Server Name Indicator)
  - IP reputation exceptions by geolocation
  - Anti-defacement file filter

See [Event on page 19](#).

- **Content routing and server pool information in attack and traffic log messages** — Traffic and attack log messages now identify both any HTTP content routing policy FortiWeb applied to the traffic and the server pool FortiWeb routed the traffic to. See [Header & body fields on page 5](#).
- **Shorter msg field when disk log is full**— The `msg` log field now has the lowest priority in the disk log. When the total size of all the log fields exceeds the disk log size limit, FortiWeb truncates the msg field, which helps preserve other log information.
- **Time offset calculation** — To improve the accuracy of log search results, FortiWeb now uses the time zone attribute to determine an absolute time offset when it is indexing messages.
- **Attack logs**
  - **HTTP protocol constraint attack log message**— The attack log message that FortiWeb generates when traffic violates a HTTP protocol constraint now provides more information about the violation, including the name of the protection profile that applied the constraint, the specific constraint, and details such as the allowed and detected values.
  - **Cookie poisoning attack log message**— The attack log message that FortiWeb generates when it detects cookie poisoning now shows the expected cookie value and actual value. In addition, it provides the cookie path and domain information.

# How to interpret FortiWeb logs

This section explains the composition of FortiWeb log messages.

In some cases, to avoid flooding attack logs with entries, FortiWeb collects multiple attack log messages into a single message. See [Attack on page 388](#).

## Header & body fields

Each log message is comprised of several field-value pairs. (The names may vary slightly between **Raw** versus **Formatted** views in the web UI.)

**ID (log\_id) header field and its value**

### Formatted view

#	ID	Sub Type
(6)		DDOS based on source IP
1	00070038	DDOS based on source IP
2	00070038	DDOS based on source IP
3	00070038	DDOS based on source IP
4	00070038	DDOS based on source IP
5	00070038	DDOS based on source IP
6	00070038	DDOS based on source IP
(24)		waf_signature_detection
7	00070010	waf_signature_detection

### Raw format

log\_id=0104012345

Field name

Field value

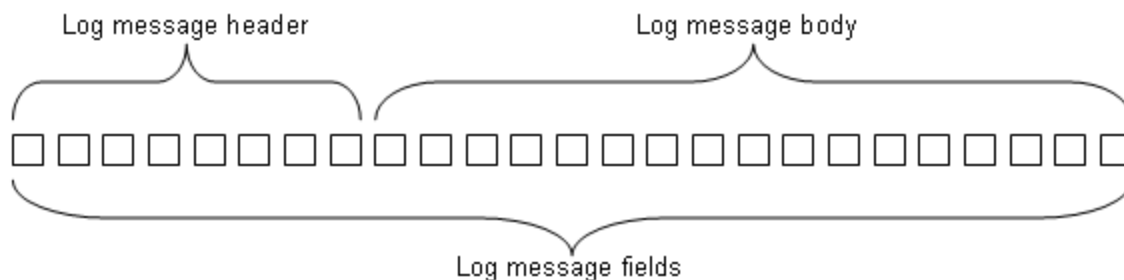
All log messages' fields belong to one of two parts:

- **Header** — Contains the time and date the log originated, a log identifier, a message identifier, the administrative domain (ADOM), the type of log, the severity level (priority) and where the log message originated. **These fields exist in all logs.**
- **Body** — Describes the reason why the log was created, plus any actions that the FortiWeb appliance took to respond to it. **These fields vary by log type.**

### Log message header and body

For example, this is a raw-format event log message. Body fields are in **bold**.

```
date=2013-10-07 time=11:30:53 log_id=10000017 m
```



```
sg_id=000000001117 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern
Time(US & Canada)" type=event subtype="system" pri=information trigger_policy=""
user=admin ui=GUI action=login status=success msg="User admin login successfully
from GUI(172.20.120.47)"
```

This attack log message contains the same header fields, but its body fields are different.

```
date=2014-06-22 time=23:52:38 log_id=20000010 msg_id=000000102972 device_id=FV-
1KD3A14800059 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=attack
subtype="waf_signature_detection" pri=alert trigger_policy="" severity_level=Low
proto=tcp service=http action=Alert policy="Auto-policy" src=10.0.8.103 src_
port=1114 dst=10.20.8.22 dst_port=80 http_method=get http_url="/" http_
host="10.0.8.22" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; "
http_session_id=none msg="[Signatures name: FWB_server_protection] [main class
name: Information Disclosure] [sub class name: HTTP Header Leakage]: 080200004"
signature_subclass="HTTP Header Leakage" signature_id="080200004"
srccountry="Reserved" content_switch_name="none" server_pool_name="Auto-ServerFarm"
```

Similarly, traffic log body fields are different.

```
date=2014-06-26 time=00:43:37 log_id=30000000 msg_id=000001351251 device_id=FV-
1KD3A14800059 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=traffic
subtype="http" pri=notice proto=tcp service=http status=success reason=none
policy=Auto-policy src=10.0.8.103 src_port=8142 dst=10.20.8.22 dst_port=80 http_
request_time=0 http_response_time=0 http_request_bytes=444 http_response_bytes=401
http_method=get http_url="/" http_host="10.0.8.22" http_agent="Mozilla/4.0
(compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR
2.0.50727; .NET CLR 3.0.4506.2152; " http_retcode=200 msg="HTTP GET request from
10.0.8.103:8142 to 10.20.8.22:80" srccountry="Reserved" content_switch_name="testa"
server_pool_name="Auto-ServerFarm"
```

The following table describes each possible header or body field, according to its name as it appears in the **Formatted** or **Raw** view.

## Log message fields

Field name  (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair  (Raw view)
		Event	Attack	Traffic	
Header					
Date  (date)	The year, month, and day when the log message was recorded.	+	+	+	date=2013-10-08
Time  (time)	The hour (according to a 24-hour clock, where 15:00 is 3:00 PM), minute, and second that the log message was recorded.	+	+	+	time=15:38:01
ID  (log_id)	See <a href="#">Log ID numbers on page 15</a> .	+	+	+	log_id=00041101
MSG ID  (msg_id)	See <a href="#">Message IDs on page 17</a> .	+	+	+	msg_id=000000000153
Device ID  (device_id)	The identifier, typically the serial number, of the appliance which originally recorded the log.	+	+	+	device_id=FV-1KD2B34567890
ADOM  (vd)	The administrative domain (ADOM) in which the log message was recorded	+	+	+	vd="root"
Time Zone  (timezone)	The name, geographical region, and Greenwich Mean Time (GMT) adjustment of the time zone in which the appliance is located.	+	+	+	timezone="(GMT-5:00) Eastern Time (US & Canada)"
Type  (type)	See <a href="#">Types on page 16</a> .	+	+	+	type=event
Sub Type  (subtype)	See <a href="#">Subtypes on page 16</a> .	+	+	+	subtype=admin

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traffic	
Level (pri)	See <a href="#">Priority level on page 16</a> .	+	+	+	pri=alert
<b>Body</b>					
Protocol (proto)	tcp  The protocol used by web traffic. By definition, for FortiWeb, this is always TCP.	-	+	+	proto=tcp
Service (service)	http or https  The name of the application-layer protocol used by the traffic. By definition, for FortiWeb, this is always HTTP or HTTPS.	-	+	+	service=http
Source (src)	The IP address of the traffic's origin.  The source varies by the direction: <ul style="list-style-type: none"> <li>• In HTTP requests, this is the web browser or other client.</li> <li>• In HTTP responses, this is the physical server.</li> </ul>	-	+	+	src=10.0.0.0
Source Port (src_port)	The port number of the traffic's origin.	-	+	+	src_port=3471



Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traff-ic	
Destination (dst)	<p>The IP address of the traffic's destination.</p> <p>The source varies by the direction:</p> <ul style="list-style-type: none"> <li>• In HTTP requests, this is the physical server.</li> <li>• In HTTP responses, this is the web browser or other client.</li> </ul>	—	+	+	dst=10.0.0.1
Destination Port (dst_port)	The port number of the traffic's destination.	—	+	+	dst_port=8080
Policy (policy)	The name of the server policy governing the traffic which caused the log message.	—	+	+	policy="policy1"
User (user)	The daemon or name of the administrator account that performed the action that caused the log message.	+	—	—	user=admin

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traffic	
User Interface (ui)	<p>The type of management interface used by the administrative session which caused the log message. Either:</p> <ul style="list-style-type: none"> <li>• GUI</li> <li>• sshd</li> <li>• telnet</li> <li>• console</li> <li>• none</li> </ul> <p>Unless the user is a daemon (which don't have a user interface), logins from <code>none</code> indicate that an administrator used the JavaScript <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.</p> <p>Logins from <code>console</code> indicate use of CLI via the local serial console port.</p>	+	-	-	ui=GUI
Action (action)	<p>The action associated with the log message or policy violation, such as:</p> <p>login or Alert</p>	+	+	-	action=Alert
Status (status)	The result of the action.	+	-	+	status=failure

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traffic	
Reason (reason)	The reason for the status, if any.	+	-	+	reason=name_invalid
Return Code (http_retcode)	The HTTP return code. If FortiWeb is configured to redirect, this is the rewritten code, <b>not</b> the original one from the server.	-	-	+	http_retcode=200
Request Time (http_request_time)	The amount of time it took FortiWeb to process the client request, in milliseconds (ms).	-	-	+	http_request_time=10
Response Time (http_response_time)	The amount of processing time for the response in milliseconds (ms). This can be a useful measure of performance issues, especially if processing involves regular expressing matching.	-	-	+	http_response_time=10
Request Bytes (http_request_bytes)	The size of the request in bytes.	-	-	+	http_request_bytes=2
Response Bytes (http_response_bytes)	The size of the individual response in bytes (B). For chunked responses, this is for each reply; it does <b>not</b> aggregate all related chunks.	-	-	+	http_response_bytes=136
Method (http_method)	The method, such as GET or POST, used by the HTTP request.	-	+	+	http_method=get

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traffic	
URL (http_url)	<p>The URL in the HTTP header of the original HTTP request, such as:</p> <pre>/images/buttons/hintOver.png</pre> <p>This does not include the service (http://) nor host name (example.nl). If FortiWeb is configured to rewrite the URL, this is the original URL from the client, <b>not</b> the rewritten one.</p>	-	+	+	http_url="/image/up.png"
Host (http_host)	<p>The <code>Host:</code> field in the HTTP header of the HTTP request, such as:</p> <pre>www.example.com</pre> <p>or</p> <pre>10.0.0.1:8080</pre> <p>This is typically a fully qualified domain name (FQDN) or IP address and port number that resolves or routes to the virtual server on the FortiWeb appliance.</p> <p>This may be different from your internal DNS name (if any) for the web server, or, if you are using HTTP <code>Host:</code> rewrites, different from the virtual host on the web server. For example, this might be <code>www.example.co.jp</code> instead of <code>www1.local</code> or the virtual host that serves responses for all DNS names, <code>www.example.com</code>.</p>	-	+	+	http_host="example.com"

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traffic	
User Agent (http_agent)	The name and version of the HTTP client, usually a web browser. This is reported by the client itself in the <code>User-Agent</code> : HTTP header. In attacks, it is often fake.	-	+	+	<code>http_agent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari-i/537.36"</code>
FortiWeb Session ID (http_session_id)	The session identifier for a client's related HTTP requests (if any).  The ID may be <code>unknown</code> if the <b>Session Management</b> option is not enabled in the applied protection profile, and therefore FortiWeb has not injected a session cookie nor inferred a session ID from the protected web application.	-	+	-	<code>http_session_id=K8BXT3TNYUM710UEGWC8IQBT-PX9PRWHB</code>
Severity Level (severity_level)	The severity that the administrator configured in the rule or policy governing the traffic which caused the log message.	-	+	-	<code>severity_level=High</code>
Trigger Policy (trigger_policy)	The name of the notification servers used to record and/or deliver this log message (if any).  The trigger policy value may be an empty string if no trigger policy was selected.	+	+	-	<code>trigger_policy=notification-server-group1</code>

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traff-ic	
Signature Subclass (signature_subclasses)	The name of the signature subclass.  If the current signature has no subclass, the main class is displayed.	-	+	-	"Cross Site Scripting"
Signature ID (signature_id)	The ID of the specific signature within the subclass that triggered the log message.	-	+	-	"010000001"
Source Country (srccountry)	The country that is the source of the traffic.	-	+	+	"United States"
Message (msg)	Details describing the reason why the log message was created.  The message varies by the nature of the cause.  The <code>msg</code> log field has the lowest priority in the disk log. When the total size of all the log fields exceeds the disk log size limit, FortiWeb truncates the <code>msg</code> field, which helps preserve other log information.	+	+	+	msg="User admin changed dns from GUI (172.20.120.47) "

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traffic	
HTTP Content Routing (content_switch_name)	The name of the associated HTTP content routing policy.	-	+	+	content_switch_name="httproutes1"
Server Pool (server_pool_name)	The name of the server pool in the associated server policy.	-	+	+	server_pool_name="Auto-ServerFarm"
Detailed Information (N/A)	<p>This column contains the entire log message in raw format.</p> <p>If your <b>Column Settings</b> show this column, the entire raw log message will be included in the row under this column, next to the formatted column view of the same log message. This way, if you want to view the entire raw log message, you can simply scroll the page, instead of switching the entire page back and forth from <b>Raw</b> to <b>Formatted</b> log views.</p> <p>This column appears only when using the <b>Formatted</b> log view. It does not actually exist as a field in the raw logs.</p>	+	+	+	date=2013-10-10 time=e=00:38:58 log_id=20000051 msg_id=000000000008...

## Log ID numbers

The **ID** (`log_id`) is an 8-digit field located in the header, immediately following the time and date fields.

The `log_id` field is a number assigned to all permutations of the same message. It classifies a log message by the nature of the cause of the log message, such as administrator authentication failures or traffic. Other log messages that share the same cause will share the same `log_id`.

For example, creating an administrator account always has the log ID `00003401`.

## Types

Each log message contains a **Type** (`type`) field that indicates its category, and in which log file it is stored.

FortiWeb appliances can record the following categories of log messages:

### Log types

Log type	Description
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.
Traffic	Records traffic flow information, such as an HTTP/HTTPS request and its response, if any.
Attack	Records attack and intrusion attempts.



Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. **Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.**

## Subtypes

Each log message contains a **Sub Type** (`subtype`) field that further subdivides its category according to the feature involved with the cause of the log message.

For example:

- In event logs, some may have a `subtype` of `admin`, `system`, or other subtypes.
- In attack logs, some may have a `subtype` of `waf_padding_oracle` or other subtypes.
- In traffic logs, the `subtype` is always `http` even if the service is HTTPS.

## Priority level

Each log message contains a **Level** (`pri`) field that indicates the estimated severity of the event that caused the log message, such as `pri=warning`, and therefore how high a priority it is likely to be.





Level (`pri`) associations with the descriptions below are not always uniform. They also may not correspond with **your own** definitions of how severe each event is. If you require notification when a specific event occurs, either configure SNMP traps or alert email by administrator-defined Severity Level (`severity_level`) or ID (`log_id`), **not** by Level (`pri`).

### Approximate log priority levels

Level (0 is highest)	Name	Description
0	Emergency	The system has become unusable.
1	Alert	Immediate action is required. <b>Used in attack logs.</b>
2	Critical	Functionality is affected.
3	Error	An error condition exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notification	Information about normal events. <b>Used in traffic logs, and in event logs for administrator logins, time changes, and normal daemon actions.</b>
6	Information	General information about system operations. <b>Used in event logs for configuration changes.</b>

For each location where the FortiWeb appliance can store log files (disk, memory, Syslog or FortiAnalyzer), you can define a severity threshold. The FortiWeb appliance will store all log messages equal to or exceeding the log severity level you select.

For example, if you select **Error**, the FortiWeb appliance will store log messages whose log severity level is **Error**, **Critical**, **Alert**, and **Emergency**.



Avoid recording log messages using low log severity thresholds such as information or notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

## Message IDs

The **MSG ID** (`msg_id`) field is an 12-digit number located in the header, incremented with each individual log message generated by the FortiWeb appliance. It is used only for numbering each entry in the database, and does not necessarily reflect its cause.

Each `msg_id` number is a unique identifier for that specific log entry. No other log messages, regardless of cause, share the same `msg_id`.

# Event

Event log messages record subsystem events such as NTP-based time changes, reboots and RAID level changes. They also record configuration changes.

Unless noted as otherwise in each event log's description:

- **Level** (`pri`) field is `information`
- **User** (`user`) field is the name of the administrator account that caused the event
- **User Interface** (`ui`) field is according to [User Interface on page 10](#)

To go to a sample, additional information, and solution (if applicable) for an event log message, click the **ID** (`log_id`) field in the table.

## Event logs by subtype & ID

ID ( <code>log_id</code> )	Sub Type ( <code>subtype</code> )
<a href="#">00001002</a>	admin
<a href="#">00001012</a>	admin
<a href="#">00001052</a>	admin
<a href="#">00001062</a>	admin
<a href="#">00002202</a>	admin
<a href="#">00002801</a>	admin
<a href="#">00002802</a>	admin
<a href="#">00002811</a>	admin
<a href="#">00003401</a>	admin
<a href="#">00003402</a>	admin
<a href="#">00003411</a>	admin
<a href="#">00004401</a>	admin
<a href="#">00004402</a>	admin
<a href="#">00004411</a>	admin

ID (log_id)	Sub Type (subtype)
00004902	admin
00006001	admin
00006002	admin
00006011	admin
00006102	admin
00006202	admin
00006302	admin
00006501	admin
00006502	admin
00006511	admin
00007302	admin
00007402	admin
00008101	admin
00008102	admin
00008111	admin
00008602	admin
00008701	admin
00008702	admin
00008711	admin
00008801	admin
00008811	admin
00008901	admin

ID (log_id)	Sub Type (subtype)
00008911	admin
00009001	admin
00009011	admin
00009101	admin
00009111	admin
00009201	admin
00009211	admin
00009301	admin
00009311	admin
00009401	admin
00009402	admin
00009411	admin
00009501	admin
00009502	admin
00009511	admin
00009702	admin
00010001	admin
00010002	admin
00010011	admin
00010201	admin
00010202	admin
00010211	admin

ID (log_id)	Sub Type (subtype)
00010401	admin
00010402	admin
00010411	admin
00010501	admin
00010502	admin
00010511	admin
00010601	admin
00010602	admin
00010611	admin
00010701	admin
00010711	admin
00020088	admin
00020201	admin
00020202	admin
00020211	admin
00020301	admin
00020302	admin
00020311	admin
00020801	admin
00020802	admin
00020811	admin
00020901	admin

ID (log_id)	Sub Type (subtype)
00020902	admin
00020911	admin
00021002	admin
00021102	admin
00021140	admin
00021202	admin
00021302	admin
00021402	admin
00022997	admin
00030001	admin
00030002	admin
00030011	admin
00032006	admin
00040001	admin
00040002	admin
00040011	admin
00040301	admin
00040302	admin
00040311	admin
00040501	admin
00040502	admin
00040511	admin

ID (log_id)	Sub Type (subtype)
00040601	admin
00040611	admin
00040623	admin
00040751	admin
00040752	admin
00040761	admin
00040801	admin
00040802	admin
00040811	admin
00040901	admin
00040902	admin
00040911	admin
00041001	admin
00041002	admin
00041011	admin
00041101	admin
00041102	admin
00041111	admin
00041201	admin
00041202	admin
00041211	admin
00041302	admin



ID (log_id)	Sub Type (subtype)
00041401	admin
00041402	admin
00041411	admin
00041601	admin
00041602	admin
00041611	admin
00041801	admin
00041802	admin
00041811	admin
00043001	admin
00043002	admin
00043011	admin
00044001	admin
00044002	admin
00044011	admin
00044401	admin
00044411	admin
00044501	admin
00044502	admin
00044511	admin
00046001	admin
00046002	admin

ID (log_id)	Sub Type (subtype)
00046011	admin
00050001	admin
00050002	admin
00050011	admin
00050201	admin
00050202	admin
00050211	admin
00050401	admin
00050402	admin
00050411	admin
00051001	admin
00051002	admin
00051011	admin
00051201	admin
00051202	admin
00051211	admin
00051401	admin
00051402	admin
00051411	admin
00051601	admin
00051602	admin
00051611	admin

ID (log_id)	Sub Type (subtype)
00051801	admin
00051802	admin
00051811	admin
00052201	admin
00052202	admin
00052211	admin
00052401	admin
00052402	admin
00052411	admin
00052601	admin
00052602	admin
00052611	admin
00053201	admin
00053202	admin
00053211	admin
00053701	admin
00053711	admin
00053901	admin
00053902	admin
00053911	admin
00054401	admin
00054402	admin

ID (log_id)	Sub Type (subtype)
00054411	admin
00054601	admin
00054602	admin
00054611	admin
00054801	admin
00054802	admin
00054811	admin
00055301	admin
00055302	admin
00055311	admin
00055501	admin
00055502	admin
00055511	admin
00055701	admin
00055702	admin
00055711	admin
00055901	admin
00055902	admin
00055911	admin
00056401	admin
00056402	admin
00056411	admin

ID (log_id)	Sub Type (subtype)
00056601	admin
00056602	admin
00056611	admin
00058601	admin
00058602	admin
00058611	admin
00059801	admin
00059802	admin
00059811	admin
00060001	admin
00060002	admin
00060011	admin
00060201	admin
00060202	admin
00060211	admin
00061201	admin
00061202	admin
00061211	admin
00061401	admin
00061402	admin
00061411	admin
00061801	admin

ID (log_id)	Sub Type (subtype)
00061802	admin
00061811	admin
00062001	admin
00062002	admin
00062011	admin
00062201	admin
00062202	admin
00062211	admin
00062401	admin
00062402	admin
00062411	admin
00063401	admin
00063402	admin
00063411	admin
00064401	admin
00064402	admin
00064411	admin
00065002	admin
00065501	admin
00065502	admin
00065511	admin
00068001	admin

ID (log_id)	Sub Type (subtype)
00068002	admin
00068011	admin
00068301	admin
00068302	admin
00068311	admin
00068401	admin
00068402	admin
00068411	admin
00068701	admin
00068711	admin
00068801	admin
00068802	admin
00068811	admin
00090001	admin
00090002	admin
00090011	admin
00090101	admin
00090102	admin
00090111	admin
00091101	admin
00091102	admin
00091111	admin

ID (log_id)	Sub Type (subtype)
00093001	admin
00093002	admin
00093011	admin
00093501	admin
00093502	admin
00093511	admin
10000009	system
10000010	system
10000011	system
10000012	system
10000013	system
10000014	system
10000015	system
10000016	system
10000017	system
10000018	system
10000019	system
10000020	system
10000021	system
10000022	system
10000023	system
10000027	system



ID (log_id)	Sub Type (subtype)
10000028	system
11001008	system
11002003	system
11002004	system
11003601	system
11004002	system
11004601	system
11004602	system
11004603	system
11004605	system
11004606	system
11004608	system
11005901	system
11006004	system
11006005	system
11006006	system
11006701	system
19999496	system
19999497	system
19999498	system

## Reboot, shut down, & boot up messages

When FortiWeb is shutting down, if you are attached to the local console, the appliance outputs messages output to the CLI notifying you that the operating system is halting, such as:

```
The system is going down NOW !!
```

or:

```
System is rebooting...
```

As one of its final actions, if logging is enabled, FortiWeb records the shutdown ([10000011](#)) or reboot ([10000010](#)) in the event log. When FortiWeb starts up again, the local console displays:

```
System is started.
```

and it records the startup ([10000009](#)). Its subsystems are loaded and readied to do their work. At this time FortiWeb records daemon startups in the event log, such as [10000023](#) and [11001008](#).

**Related**

- [10000009](#)
- [10000010](#)
- [10000011](#)
- [10000023](#)
- [11001008](#)

## 00001002

### Meaning

Either:

- An administrator changed the NTP synchronization interval.
- An administrator changed the time zone setting.

Field name	Description
<b>ID</b>	00001002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Level</b>	notification or information
(pri)	See <a href="#">Priority level on page 16</a> .

### Examples

```
date=2014-04-09 time=22:11:33 log_id=00001002 msg_id=000000192626 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed a time setting from GUI(172.22.6.240) "
```

### Related

- [00021140](#)
- [00006102](#)

## 00001012

### Meaning

A FortiWeb administrator changed the host name of the appliance.

Field name	Description
<b>ID</b>	00001012
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Level</b>	notification or information (changing the idle GUI session timeout)
(pri)	See <a href="#">Priority level on page 16</a> .

### Examples

```
date=2014-04-10 time=12:11:17 log_id=00001012 msg_id=000000192621 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed hostname global setting FortiWeb to 1KD_1 from GUI (172.22.6.240) "
```

### Related

- [00001002](#)

## 00001052

### Meaning

An administrator changed the idle GUI session timeout.

Field name	Description
<b>ID</b>	00001052
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Level</b>	notification or information (changing the idle GUI session timeout)
(pri)	See <a href="#">Priority level on page 16</a> .

### Examples

```
date=2014-04-10 time=12:10:51 log_id=00001052 msg_id=000000192620 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed idle GUI session timeout from GUI(172.22.6.240)"
```

### Related

- [00001002](#)

## 00001062

### Meaning

An administrator changed the listening/source port for configuration synchronization with another FortiWeb.

Field name	Description
<b>ID</b>	00001062
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Level</b>	notice
(pri)	See <a href="#">Priority level on page 16</a> .

### Examples

```
date=2014-09-10 time=22:16:40 log_id=00001062 msg_id=000003041952 device_
id=FV400C3M14000006 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event
subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit
status=success msg="User admin changed sync-port global setting 8333 to 1111 from GUI
(172.22.14.6) "
```

### Related

- [00001002](#)

## 00002202

### Meaning

A FortiWeb administrator changed a setting in **System > Config > Advanced** on the appliance.

Field name	Description
<b>ID</b>	00002202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:43:22 log_id=00002202 msg_id=0000000000042 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed advanced from GUI(172.20.120.47) "
```

## 00002801

### Meaning

A FortiWeb administrator created an administrator access profile.

Field name	Description
<b>ID</b>	00002801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:43:04 log_id=00002801 msg_id=0000000000041 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added accprofile read-only from GUI
(172.20.120.47) "
```

### Related

- [00002802](#)
- [00002811](#)
- [00003401](#)



## 00002802

### Meaning

A FortiWeb administrator changed an administrator access profile.

Field name	Description
<b>ID</b>	00002802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:43:14 log_id=00002802 msg_id=0000000000042 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed accprofile read-only from GUI
(172.20.120.47) "
```

### Related

- [00002801](#)
- [00002811](#)
- [00003401](#)

## 00002811

### Meaning

A FortiWeb administrator deleted an administrator access profile.

Field name	Description
<b>ID</b>	00002811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:43:34 log_id=00002811 msg_id=0000000000045 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=delete status=success msg="User admin deleted accprofile read-only from GUI
(172.20.120.47) "
```

### Related

- [00002801](#)
- [00002802](#)
- [00003401](#)

## 00003401

### Meaning

A FortiWeb administrator created an administrator account.

Field name	Description
<b>ID</b>	00003401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:45:44 log_id=00003401 msg_id=0000000000048 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added admin admin1 from GUI(172.20.120.47) "
```

### Related

- [00003402](#)
- [00003411](#)
- [00002801](#)
- [00004402](#)
- [00010201](#)
- [00010401](#)
- [00010701](#)

## 00003402

### Meaning

A FortiWeb administrator changed an administrator account. This can include resetting the account's password.

### Field name

### Description

**ID**

00003402

(log\_id)

See [Log ID numbers on page 15](#).

### Examples

```
date=2013-10-08 time=09:45:44 log_id=00003402 msg_id=0000000000049 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed admin admin1 from GUI
(172.20.120.47) "
```

### Related

- [00003401](#)
- [00003411](#)
- [00002801](#)
- [00010201](#)
- [00010401](#)
- [00010701](#)

## 00003411

### Meaning

A FortiWeb administrator deleted an administrator account.

Field name	Description
<b>ID</b>	00003411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:46:44 log_id=00003411 msg_id=0000000000052 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=delete status=success msg="User admin deleted admin admin1 from GUI
(172.20.120.47) "
```

### Related

- [00003401](#)
- [00003402](#)
- [00002801](#)

## 00004401

### Meaning

A FortiWeb administrator created a VLAN subinterface or link aggregate.

Field name	Description
<b>ID</b>	00004401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-06 time=11:00:13 log_id=00004401 msg_id=000000001083 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console
action=add status=success msg="User admin added interface vlan3 from console"
```

### Related

- [00004402](#)
- [00030001](#)
- [00030011](#)
- [11006004](#)

## 00004402

## Meaning

A FortiWeb administrator changed the IP address or allowed administrative access protocols of a network interface. This does **not** include bringing up or bringing down the interface (see [11006004](#)).

Field name	Description
<b>ID</b> (log_id)	00004402  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	admin  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI   none   telnet   ssh   console}  Logins from jsconsole indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Message</b> (msg)	User <administrator_name> changed interface <interface_name> from {GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

## Examples

```
date=2013-10-06 time=11:00:19 log_id=00004402 msg_id=000000001085 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit status=success msg="User admin changed interface port1 from console"
```

**Related**

- [00003401](#)
- [00004401](#)
- [00006202](#)
- [00030001](#)
- [00030011](#)
- [11006004](#)



## 00004411

## Meaning

A FortiWeb administrator deleted a VLAN subinterface or link aggregate.

Field name	Description
<b>ID</b> (log_id)	00004411  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	admin  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI   none   telnet   ssh   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Message</b> (msg)	User <administrator_name> changed interface <interface_name> from {GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

## Examples

```
date=2013-10-06 time=11:00:19 log_id=00004411 msg_id=000000001089 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=delete status=success msg="User admin deleted interface aggl from console"
```

## Related

- [00004401](#)
- [00004402](#)

- [00030001](#)
- [00030011](#)
- [11006004](#)

## 00004902

## Meaning

A FortiWeb administrator changed the operation mode.

Field name	Description
<b>ID</b> (log_id)	00004902  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	admin  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Message</b> (msg)	User <administrator_name> changed settings from {GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

## Examples

```
date=2014-05-14 time=18:05:27 log_id=00004902 msg_id=000000021625 device_id=FV-3KC3R10700108 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed settings from GUI(172.22.6.241)"
```

## Related

- [00006001](#)

## 00006001

## Meaning

A FortiWeb administrator created a bridge ("V-Zone").

Field name	Description
<b>ID</b> (log_id)	00006001  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}
<b>Message</b> (msg)	User <administrator_name> added V-Zone <bridge_name> from {GUI(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

## Examples

```
date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event
subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin
added V-Zone bridge1 from GUI(172.20.120.229)."
```

## Related

- [00006002](#)
- [00006011](#)

## 00006002

**Meaning**

A FortiWeb administrator changed a bridge ("V-Zone").

Field name	Description
<b>ID</b> (log_id)	00006002  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}
<b>Message</b> (msg)	User <administrator_name> modified V-Zone <bridge_name> from {GUI(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

**Examples**

```
date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event
subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin
modified V-Zone bridge1 from GUI(172.20.120.229)."
```

**Related**

- [00006001](#)
- [00006011](#)

## 00006011

**Meaning**

A FortiWeb administrator deleted a bridge ("V-Zone").

Field name	Description
<b>ID</b> (log_id)	00006011  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}
<b>Message</b> (msg)	User <administrator_name> deleted V-Zone <bridge_name> from {GUI(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}.

**Examples**

```
date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event
subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin
deleted V-Zone bridge1 from GUI(172.20.120.229)."
```

**Related**

- [00006001](#)
- [00006002](#)

## 00006102

### Meaning

A FortiWeb administrator changed the IP address of the configuration synchronization peer.

Field name	Description
<b>ID</b>	00006102
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:47:28 log_id=00006102 msg_id=0000000000060 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed conf-sync from GUI(172.20.120.47) "
```

### Related

- [00001002](#)

## 00006202

### Meaning

A FortiWeb administrator changed the DNS settings.

Field name	Description
<b>ID</b>	00006202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:47:37 log_id=00006202 msg_id=0000000000061 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed dns from GUI(172.20.120.47)"
```

### Related

- [00004402](#)
- [00030011](#)



## 00006302

### Meaning

A FortiWeb administrator changed the system-wide SNMP settings such as the description, location, or contact information.

Field name	Description
<b>ID</b>	00006302
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:44:37 log_id=00006302 msg_id=0000000000044 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed snmpsysinfo from GUI(172.20.120.47)
"
```

### Related

- [00004402](#)
- [00006501](#)

## 00006501

### Meaning

A FortiWeb administrator added an SNMP community.

Field name	Description
<b>ID</b>	00006501
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:45:04 log_id=00006501 msg_id=0000000000045 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added snmp community 1 from GUI
(172.20.120.47) "
```

### Related

- [00004402](#)
- [00006302](#)
- [00006502](#)
- [00006511](#)

## 00006502

### Meaning

A FortiWeb administrator changed an SNMP community setting such as the SNMP manager and trap events.

Field name	Description
<b>ID</b>	00006502
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:45:04 log_id=00006502 msg_id=0000000000046 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed snmp community 1 from GUI
(172.20.120.47) "
```

### Related

- [00004402](#)
- [00006302](#)
- [00006501](#)
- [00006511](#)

## 00006511

### Meaning

A FortiWeb administrator deleted an SNMP community.

Field name	Description
<b>ID</b>	00006511
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:47:11 log_id=00006511 msg_id=0000000000059 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted snmp community 2 from GUI
(172.20.120.47) "
```

### Related

- [00004402](#)
- [00006302](#)
- [00006501](#)
- [00006502](#)

## 00007302

### Meaning

A FortiWeb administrator changed the setting that overrides the default Fortiguard Distribution Server (FDS).

Field name	Description
<b>ID</b>	00007302
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=00:15:13 log_id=00007302 msg_id=000000070586 device_id=FV-1KC3R10700031 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-autoupdate-override from GUI (172.22.6.237) "
```

### Related

- [00007402](#)

## 00007402

### Meaning

A FortiWeb administrator changed the configuration that determines how the FortiWeb appliance accesses the Fortinet Distribution Network (FDN) to retrieve updates.

Field name	Description
<b>ID</b>	00007402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:19:36 log_id=00007402 msg_id=000000734625 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-autoupdate-schedule from GUI (172.22.6.237) "
```

### Related

- [00007302](#)

## 00008101

### Meaning

A FortiWeb administrator created a schedule for a periodic configuration backup to an FTP/SFTP server.

Field name	Description
<b>ID</b>	00008101
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:42:14 log_id=00008101 msg_id=0000000000037 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added backup scheduled_backup from GUI
(172.20.120.47) "
```

### Related

- [00004402](#)
- [00008102](#)
- [00008111](#)

## 00008102

### Meaning

A FortiWeb administrator changed a schedule for a periodic configuration backup to an FTP/SFTP server.

Field name	Description
<b>ID</b>	00008102
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:42:24 log_id=00008102 msg_id=0000000000038 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed backup scheduled_backup from GUI
(172.20.120.47) "
```

### Related

- [00004402](#)
- [00008101](#)
- [00008111](#)



## 00008111

### Meaning

A FortiWeb administrator deleted a schedule for a periodic configuration backup to an FTP/SFTP server.

Field name	Description
<b>ID</b>	00008111
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:42:54 log_id=00008111 msg_id=0000000000040 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted backup scheduled_backup from GUI
(172.20.120.47) "
```

### Related

- [00004402](#)
- [00008101](#)
- [00008102](#)

## 00008602

### Meaning

A FortiWeb administrator changed a TCP `SYN` flood denial of service (DoS) setting.

Field name	Description
<b>ID</b>	00008602
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:38:51 log_id=00008602 msg_id=000000000174 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed dos-prevention from GUI
(172.20.120.47) "
```

## 00008701

### Meaning

A FortiWeb administrator uploaded a locally stored server certificate and (if applicable) private key.

Field name	Description
<b>ID</b>	00008701
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:42:13 log_id=00008701 msg_id=0000000000039 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added local certificate-with-key from GUI
(172.20.120.47) "
```

### Related

- [00008702](#)
- [00008711](#)

## 00008702

### Meaning

A FortiWeb administrator changed the description of a locally stored server certificate and private key.

Field name	Description
<b>ID</b>	00008702
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:42:53 log_id=00008702 msg_id=0000000000040 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed local certificate-with-key from GUI
(172.20.120.47) "
```

### Related

- [00008701](#)
- [00008711](#)

## 00008711

### Meaning

A FortiWeb administrator deleted a locally stored server certificate and (if applicable) private key.

Field name	Description
<b>ID</b>	00008711
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=09:42:59 log_id=00008711 msg_id=0000000000041 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted local certificate-with-key from GUI
(172.20.120.47) "
```

### Related

- [00008701](#)
- [00008702](#)

## 00008801

### Meaning

A FortiWeb administrator added a configuration for a certificate of the HTTP CRL server of your certificate authority (CA).

Field name	Description
------------	-------------

<b>ID</b>	00008801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:01:21 log_id=00008801 msg_id=000000179544 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added remote REMOTE_Cert_2 from GUI
(172.22.6.66) "
```

### Related

- [00008811](#)
- [00009301](#)
- [00009311](#)
- [11006701](#)

## 00008811

### Meaning

A FortiWeb administrator deleted a configuration for a certificate of the HTTP CRL server of your certificate authority (CA).

### Field name

### Description

**ID**

00008811

(log\_id)

See [Log ID numbers on page 15](#).

### Examples

```
date=2014-04-10 time=17:02:34 log_id=00008811 msg_id=000000179545 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted remote REMOTE_Cert_2 from GUI
(172.22.6.66) "
```

### Related

- [00008801](#)
- [00009301](#)
- [00009311](#)
- [11006701](#)

## 00008901

### Meaning

A FortiWeb administrator added a certificate.

Field name	Description
<b>ID</b>	00008901
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:03:26 log_id=00008901 msg_id=000000179546 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added certificate ca CA_Cert_4 from GUI
(172.22.6.66) "
```

### Related

- [00008911](#)



## 00008911

### Meaning

A FortiWeb administrator deleted a certificate.

Field name	Description
<b>ID</b>	00008911
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:03:31 log_id=00008911 msg_id=000000179547 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted certificate ca CA_Cert_4 from GUI
(172.22.6.66) "
```

### Related

- [00008901](#)

## 00009001

### Meaning

A FortiWeb administrator added a certificate authorities (CA) group.

Field name	Description
<b>ID</b>	00009001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:06:20 log_id=00009001 msg_id=000000179548 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added certificate ca-group ca_g from GUI
(172.22.6.66) "
```

### Related

- [00009011](#)

## 00009011

### Meaning

A FortiWeb administrator deleted a certificate authorities (CA) group.

Field name	Description
<b>ID</b>	00009011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:06:31 log_id=00009011 msg_id=000000179549 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted certificate ca-group ca_g from GUI
(172.22.6.66) "
```

### Related

- [00009001](#)

## 00009101

### Meaning

A FortiWeb administrator added an intermediate CA certificate.

Field name	Description
<b>ID</b>	00009101
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:09:10 log_id=00009101 msg_id=000000179550 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added certificate intermediate-certificate
Inter_Cert_1 from GUI(172.22.6.66) "
```

### Related

- [00009111](#)

## 00009111

### Meaning

A FortiWeb administrator deleted an intermediate CA certificate.

Field name	Description
<b>ID</b>	00009111
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:09:14 log_id=00009111 msg_id=000000179551 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted certificate intermediate-certificate
Inter_Cert_1 from GUI(172.22.6.66) "
```

### Related

- [00009101](#)

## 00009201

### Meaning

A FortiWeb administrator added an intermediate CA certificate group.

Field name	Description
<b>ID</b>	00009201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:10:42 log_id=00009201 msg_id=000000179552 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added certificate intermediate-certificate-
group inter_g from GUI(172.22.6.66) "
```

### Related

- [00009211](#)

## 00009211

### Meaning

A FortiWeb administrator deleted an intermediate CA certificate group.

Field name	Description
<b>ID</b>	00009211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:10:46 log_id=00009211 msg_id=000000179553 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted certificate intermediate-
certificate-group inter_g from GUI(172.22.6.66)"
```

### Related

- [00009201](#)

## 00009301

### Meaning

A FortiWeb administrator added a certificate revocation list (CRL) configuration.

Field name	Description
<b>ID</b>	00009301
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:12:24 log_id=00009301 msg_id=000000179554 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added certificate crl CRL_4 from GUI
(172.22.6.66) "
```

### Related

- [00008801](#)
- [00008811](#)
- [00009311](#)
- [11006701](#)



## 00009311

### Meaning

A FortiWeb administrator deleted a certificate revocation list (CRL) configuration.

Field name	Description
<b>ID</b>	00009311
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:12:28 log_id=00009311 msg_id=000000179555 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted certificate crl CRL_4 from GUI
(172.22.6.66) "
```

### Related

- [00008801](#)
- [00008811](#)
- [00009301](#)
- [11006701](#)

## 00009401

### Meaning

A FortiWeb administrator added a certificate verification rule.

Field name	Description
<b>ID</b>	00009401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:15:06 log_id=00009401 msg_id=000000179559 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added certificate verify CV from GUI
(172.22.6.66) "
```

### Related

- [00009402](#)
- [00009411](#)

## 00009402

### Meaning

A FortiWeb administrator edited a certificate verification rule.

Field name	Description
<b>ID</b>	00009402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:15:11 log_id=00009402 msg_id=000000179560 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed certificate verify CV from GUI
(172.22.6.66) "
```

### Related

- [00009401](#)
- [00009411](#)

## 00009411

### Meaning

A FortiWeb administrator deleted a certificate verification rule.

Field name	Description
<b>ID</b>	00009411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:15:14 log_id=00009411 msg_id=000000179561 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted certificate verify CV from GUI
(172.22.6.66) "
```

### Related

- [00009401](#)
- [00009402](#)

## 00009501

### Meaning

A FortiWeb administrator added a Server Name Indication (SNI) configuration.

Field name	Description
<b>ID</b>	00009501
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-03 time=11:16:33 log_id=00009501 msg_id=000000003148 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add
status=success msg="User admin added certificate sni online_store from GUI
(172.20.120.61) "
```

### Related

- [00009502](#)
- [00009511](#)

## 00009502

### Meaning

A FortiWeb administrator changed a Server Name Indication (SNI) configuration.

Field name	Description
<b>ID</b>	00009502
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-03 time=11:16:33 log_id=00009502 msg_id=000000003148 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin changed certificate sni online_store from GUI (172.20.120.61) "
```

### Related

- [00009501](#)
- [00009511](#)

## 00009511

### Meaning

A FortiWeb administrator deleted a Server Name Indication (SNI) configuration.

Field name	Description
<b>ID</b>	00009511
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-03 time=11:25:07 log_id=00009511 msg_id=000000003149 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del
status=success msg="User admin deleted certificate sni online_store from GUI
(172.20.120.61) "
```

### Related

- [00009501](#)
- [00009502](#)

## 00009702

### Meaning

A FortiWeb administrator changed system-wide FortiGuard Antivirus scan settings.

Field name	Description
<b>ID</b>	00009702
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:31:09 log_id=00009702 msg_id=000000734627 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-antivirus from GUI(172.22.6.237) "
```



## 00010001

### Meaning

A FortiWeb administrator added a locally-defined account for a web site end-user.

### Field name

### Description

**ID**

00010001

(log\_id)

See [Log ID numbers on page 15](#).

### Examples

```
date=2013-10-08 time=10:01:51 log_id=00010001 msg_id=0000000000079 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added local-user user1 from GUI
(172.20.120.47) "
```

### Related

- [00010001](#)
- [00010002](#)
- [00010201](#)
- [00010401](#)
- [00010501](#)

## 00010002

### Meaning

A FortiWeb administrator changed a locally defined account for a web site end-user.

Field name	Description
<b>ID</b>	00010002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:01:56 log_id=00010002 msg_id=0000000000080 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed local-user user1 from GUI
(172.20.120.47) "
```

### Related

- [00010001](#)
- [00010011](#)
- [00010501](#)

## 00010011

### Meaning

A FortiWeb administrator deleted a locally-defined account for a web site end-user.

Field name	Description
<b>ID</b>	00010011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:01:59 log_id=00010011 msg_id=0000000000081 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted local-user user1 from GUI
(172.20.120.47) "
```

### Related

- [00010001](#)
- [00010002](#)

## 00010201

### Meaning

A FortiWeb administrator added an LDAP query.

Field name	Description
<b>ID</b>	00010201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-09 time=15:44:16 log_id=00010201 msg_id=000000000310 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added ldap-user ldap-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010202](#)
- [00010211](#)
- [00010001](#)
- [00003401](#)

## 00010202

### Meaning

A FortiWeb administrator changed an LDAP query.

Field name	Description
<b>ID</b>	00010202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-09 time=15:44:23 log_id=00010202 msg_id=000000000311 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed ldap-user ldap-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010201](#)
- [00010211](#)
- [00010001](#)
- [00003401](#)

## 00010211

### Meaning

A FortiWeb administrator deleted an LDAP query.

Field name	Description
<b>ID</b>	00010211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-09 time=15:44:32 log_id=00010211 msg_id=0000000000312 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted ldap-user ldap-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010201](#)
- [00010202](#)
- [00010001](#)
- [00003401](#)

## 00010401

### Meaning

A FortiWeb administrator created a RADIUS query.

Field name	Description
<b>ID</b>	00010401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:02:59 log_id=00010401 msg_id=0000000000082 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added radius-user radius-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010402](#)
- [00010411](#)
- [00010001](#)
- [00003401](#)

## 00010402

### Meaning

A FortiWeb administrator changed a RADIUS query.

Field name	Description
<b>ID</b>	00010402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:03:14 log_id=00010402 msg_id=0000000000083 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed radius-user radius-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010401](#)
- [00010411](#)
- [00010001](#)
- [00003401](#)



## 00010411

### Meaning

A FortiWeb administrator deleted a RADIUS query.

Field name	Description
<b>ID</b>	00010411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:03:24 log_id=00010411 msg_id=0000000000084 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted radius-user radius-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010401](#)
- [00010402](#)
- [00010001](#)
- [00003401](#)

## 00010501

### Meaning

A FortiWeb administrator added an NTLM query.

Field name	Description
<b>ID</b>	00010501
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:03:34 log_id=00010501 msg_id=0000000000085 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added ntlm-user ntlm-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010502](#)
- [00010511](#)
- [00010001](#)

## 00010502

### Meaning

A FortiWeb administrator changed an NTLM query.

Field name	Description
<b>ID</b>	00010502
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:03:44 log_id=00010502 msg_id=0000000000086 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed ntlm-user ntlm-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010501](#)
- [00010511](#)
- [00010001](#)

## 00010511

### Meaning

A FortiWeb administrator deleted an NTLM query.

Field name	Description
<b>ID</b>	00010511
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:03:54 log_id=00010511 msg_id=0000000000087 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted ntlm-user ntlm-query1 from GUI
(172.20.120.47) "
```

### Related

- [00010501](#)
- [00010502](#)
- [00010001](#)

## 00010601

### Meaning

A FortiWeb administrator added a user group.

Field name	Description
<b>ID</b>	00010601
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:04:07 log_id=00010601 msg_id=0000000000082 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added User Group user-group1 from GUI
(172.20.120.47) "
```

### Related

- [00010602](#)
- [00010611](#)
- [00010201](#)
- [00010401](#)
- [00010501](#)
- [00010001](#)

## 00010602

### Meaning

A FortiWeb administrator changed a user group.

Field name	Description
<b>ID</b>	00010602
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:06:24 log_id=00010602 msg_id=0000000000083 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed user user-group user-group1 from
GUI(172.20.120.47) "
```

### Related

- [00010601](#)
- [00010611](#)
- [00010201](#)
- [00010401](#)
- [00010501](#)
- [00010001](#)

## 00010611

### Meaning

A FortiWeb administrator deleted a user group.

Field name	Description
<b>ID</b>	00010611
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:06:34 log_id=00010611 msg_id=0000000000084 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin deleted user user-group user-group1 from
GUI(172.20.120.47) "
```

### Related

- [00010602](#)
- [00010601](#)
- [00010201](#)
- [00010401](#)
- [00010501](#)
- [00010001](#)

## 00010701

### Meaning

A FortiWeb administrator added an administrator group.

Field name	Description
<b>ID</b>	00010701
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:06:46 log_id=00010701 msg_id=0000000000085 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added user admin-group admin-query-group1
from GUI(172.20.120.47)"
```

### Related

- [00010711](#)
- [00010201](#)
- [00010401](#)
- [00003401](#)



## 00010711

### Meaning

A FortiWeb administrator deleted an administrator group.

Field name	Description
<b>ID</b>	00010711
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:06:46 log_id=00010701 msg_id=0000000000085 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin deleted user admin-group admin-query-group1
from GUI(172.20.120.47)"
```

### Related

- [00010701](#)
- [00010201](#)
- [00010401](#)
- [00003401](#)

## 00020088

**Meaning**

During a firmware upgrade, if the new firmware uses a different format for any existing settings, FortiWeb will attempt also to upgrade the configuration. If FortiWeb had to convert any settings to the new format, this log is recorded.

Normally, no action is required. However, if you notice any behavior changes after the upgrade, you may want to compare your configuration with a backup copy to verify that it has been converted correctly. This is especially true if you have not followed the upgrade path recommended in the Release Notes.

Field name	Description
<b>ID</b> (log_id)	00020088 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	unknown
<b>User Interface</b> (ui)	
<b>Action</b> (action)	upgrade
<b>Status</b> (status)	success
<b>Message</b> (msg)	The old configurations are not compatible with the new version, and some of them have been changed to be correct.

### Examples

```
date=2012-11-04 time=19:11:01 log_id=00020088 msg_id=000000853622 type=event
subtype="system" pri=information device_id=FVVM080000005545 vd="root" timezone="(GMT-
8:00)Pacific Time(US&Canada)" user=unknown ui="" action=upgrade status=success
reason=none msg="The old configurations are not compatible with the new version, and
some of them have been changed to be correct."
```

## 00020201

### Meaning

A FortiWeb administrator configured a connection to a Syslog server.

Field name	Description
<b>ID</b>	00020201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=11:43:02 log_id=00020201 msg_id=000001014451 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added syslog-policy 1 from GUI(172.22.6.231)
"
```

### Related

- [00020202](#)
- [00020211](#)

## 00020202

### Meaning

A FortiWeb administrator changed the configuration of a connection to a Syslog server.

Field name	Description
<b>ID</b>	00020202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=11:43:32 log_id=00020202 msg_id=000001014452 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed syslog-policy 1 from GUI
(172.22.6.231) "
```

### Related

- [00020201](#)
- [00020211](#)

## 00020211

### Meaning

A FortiWeb administrator deleted a connection to a Syslog server.

Field name	Description
<b>ID</b>	00020211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=11:43:42 log_id=00020211 msg_id=000001014453 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted syslog-policy 1 from GUI
(172.22.6.231) "
```

### Related

- [00020201](#)
- [00020202](#)

## 00020301

### Meaning

A FortiWeb administrator added an email policy.

Field name	Description
<b>ID</b>	00020301
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=11:37:10 log_id=00020301 msg_id=000001014448 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added mail-policy test from GUI
(172.22.6.231) "
```

### Related

- [00020302](#)
- [00020311](#)

## 00020302

### Meaning

A FortiWeb administrator made changes to an email policy.

Field name	Description
<b>ID</b>	00020302
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=11:38:20 log_id=00020302 msg_id=000001014449 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed mail-policy test from GUI
(172.22.6.231) "
```

### Related

- [00020302](#)
- [00020311](#)



## 00020311

### Meaning

A FortiWeb administrator deleted an email policy.

Field name	Description
<b>ID</b>	00020311
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=11:40:17 log_id=00020311 msg_id=000001014450 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted mail-policy test from GUI
(172.22.6.231) "
```

### Related

- [00020302](#)
- [00020311](#)

## 00020801

### Meaning

A FortiWeb administrator added a configuration that sends log messages to a remote FortiAnalyzer appliance.

Field name	Description
<b>ID</b>	00020801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=12:06:28 log_id=00020801 msg_id=000001014461 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added fortianalyzer-policy test from GUI
(172.22.6.231) "
```

### Related

- [00020802](#)
- [00020811](#)

## 00020802

### Meaning

A FortiWeb administrator made changes to a configuration that sends log messages to a remote FortiAnalyzer appliance.

Field name	Description
<b>ID</b>	00020802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=12:07:10 log_id=00020802 msg_id=000001014462 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed fortianalyzer-policy test from GUI
(172.22.6.231) "
```

### Related

- [00020801](#)
- [00020811](#)

## 00020811

### Meaning

A FortiWeb administrator deleted a configuration that sends log messages to a remote FortiAnalyzer appliance.

Field name	Description
------------	-------------

<b>ID</b>	00020811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=12:07:40 log_id=00020811 msg_id=000001014463 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted fortianalyzer-policy test from GUI
(172.22.6.231) "
```

### Related

- [00020801](#)
- [00020802](#)

## 00020901

### Meaning

A FortiWeb administrator added a trigger policy that is used by the notification process.

Field name	Description
<b>ID</b>	00020901
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=12:08:51 log_id=00020901 msg_id=000001014464 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added trigger-policy 1 from GUI
(172.22.6.231) "
```

### Related

- [00020902](#)
- [00020911](#)

## 00020902

### Meaning

A FortiWeb administrator made a change to a trigger policy that is used by the notification process.

Field name	Description
<b>ID</b>	00020902
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=12:09:39 log_id=00020902 msg_id=000001014465 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed trigger-policy 1 from GUI
(172.22.6.231) "
```

### Related

- [00020901](#)
- [00020911](#)

## 00020911

### Meaning

A FortiWeb administrator deleted a trigger policy that is used by the notification process.

Field name	Description
<b>ID</b>	00020911
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=12:10:10 log_id=00020911 msg_id=000001014466 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted trigger-policy 1 from GUI
(172.22.6.231) "
```

### Related

- [00020901](#)
- [00020902](#)

## 00021002

### Meaning

A FortiWeb administrator enabled or disabled storing logs on the appliance's hard disk.

Field name	Description
<b>ID</b>	00021002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=01:34:07 log_id=00021002 msg_id=0000000000016 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed setting for saving logs to disk from GUI"
```

### Related

- [00021302](#)



## 00021102

### Meaning

A FortiWeb administrator changed the configuration for event logging to memory (RAM).

Field name	Description
<b>ID</b>	00021102
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=12:10:52 log_id=00021102 msg_id=000001014467 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed memory from GUI(172.22.6.231)"
```

## 00021140

### Meaning

The FortiWeb's system clock was updated via NTP.

If you are using FortiWeb-VM, this message is often displayed after you unsuspend the VM.

Field name	Description
<b>ID</b>	00021140
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Level</b>	notification
(pri)	See <a href="#">Priority level on page 16</a> .
<b>User</b>	ntp_daemon
(user)	
<b>User Interface</b>	none
(ui)	

### Examples

```
date=2014-09-11 time=11:51:56 log_id=00021140 msg_id=000000133596 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=ntp_daemon ui=none action=edit status=success msg="global time setting change field:date-time The ntp daemon changed time from Wed Sep 10 20:51:48 2014 to Thu Sep 11 03:51:56 2014 "
```

### Related

- [00001002](#)

## 00021202

### Meaning

A FortiWeb administrator changed the configuration for recording attack log messages on the local FortiWeb disk.

Field name	Description
<b>ID</b>	00021202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=12:02:33 log_id=00021202 msg_id=000001014457 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed attack-log from GUI(172.22.6.231) "
```

## 00021302

### Meaning

A FortiWeb administrator enabled or disabled storing traffic logs on the appliance's hard disk.

Field name	Description
<b>ID</b>	00021302
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=01:34:51 log_id=00021302 msg_id=0000000000017 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit
status=success msg="User admin changed traffic log setting from GUI"
```

### Related

- [00021002](#)

## 00021402

### Meaning

A FortiWeb administrator made changes to the configuration for event log recording.

Field name	Description
<b>ID</b>	00021402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:48:20 log_id=00021402 msg_id=000001015952 device_
id=FV400C3M12000023 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed event-log from GUI(172.22.6.231) "
```

## 00022997

### Meaning

FortiWeb does not have enough hard disk space in order to store data gathered for auto-learning.

### Solution

If you have just updated the firmware, check the Release Notes. (Some firmware updates require that you resize the partitions before you upgrade. If you missed this step, it will cause this log message.)

If this log message is preceded by log ID [11006005](#), auto-learning data could not be stored because the data disk's file system is not currently mounted. For solutions, see [11006005](#).

Otherwise, delete any unnecessary auto-learning data, and disable it in policies where it is no longer required. This will free disk space.

Field name	Description
<b>ID</b> (log_id)	00022997  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	alert  See <a href="#">Priority level on page 16</a> .
<b>Message</b> (msg)	Disk free space is not enough for autolearn

### Examples

```
date=2012-09-27 time=07:44:00 log_id=00022997 msg_id=000000018352 type=event
subtype="system" pri=alert device_id=FV-1KC3R11700136 vd="root" timezone="(GMT-5:00)
Eastern Time (US & Canada)" msg="Disk free space is not enough for autolearn"
```

### Related

- [11006005](#)

## 00030001

### Meaning

An administrator created an IP-layer static route.

Field name	Description
<b>ID</b>	00030001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-06 time=11:03:37 log_id=00030001 msg_id=000000001086 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console
action=add status=success msg="User admin added static-route 1 from console"
```

### Related

- [00004402](#)
- [00006202](#)
- [00030002](#)
- [00030011](#)
- [00040623](#)

## 00030002

### Meaning

An administrator changed an IP-layer static route.

Field name	Description
<b>ID</b>	00030002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-06 time=11:03:47 log_id=00030002 msg_id=000000001087 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console
action=add status=success msg="User admin changed static-route 1 from console"
```

### Related

- [00004402](#)
- [00006202](#)
- [00030001](#)
- [00030011](#)
- [00040623](#)



## 00030011

### Meaning

An administrator deleted an IP-layer static route.

Field name	Description
<b>ID</b>	00030011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-06 time=11:00:12 log_id=00030011 msg_id=000000001084 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console
action=del status=success msg="User admin deleted static-route 1 from console"
```

### Related

- [00030001](#)
- [00030002](#)
- [00004402](#)
- [00040623](#)

## 00032006

### Meaning

Either:

- The maximum number of concurrent sessions has been reached. For more information on model- or configuration-dependent limits, see the *FortiWeb Administration Guide*.
- A policy was reloaded after a configuration change in order to free memory.

Field name	Description
<b>ID</b>	00032006
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	admin
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>Level</b>	information (login or daemon start) or alert (concurrent session limit reached)
(pri)	See <a href="#">Priority level on page 16</a> .
<b>Message</b>	policy <policy_name> concurrent session exceed threshold
(msg)	policy <policy_name> refreshed to free resources

### Examples

```
date=2012-10-25 time=09:31:07 log_id=00032006 msg_id=000066877877 type=event
subtype="admin" pri=alert device_id=FVVM020000003619 vd="root" timezone="(GMT)
Greenwich Mean Time: Dublin,Edinburgh,Lisbon,London" msg="policy policy1 concurrent
session exceed threshold"
```

```
date=2013-01-16 time=12:27:33 log_id=00032006 msg_id=000000201047 type=event
subtype="admin" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-
5:00)Eastern Time(US & Canada)" msg="policy policy1 refreshed to free resources"
```

### Related

- [10000014](#)

## 00040001

### Meaning

An administrator created a server availability monitor ("health check").

Field name	Description
<b>ID</b>	00040001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:14:10 log_id=00040001 msg_id=000000000105 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added health uptime-check1 from GUI
(172.20.120.47)
```

### Related

- [00040002](#)
- [00040011](#)
- [19999496](#)

## 00040002

### Meaning

An administrator changed a server availability monitor ("health check").

Field name	Description
<b>ID</b>	00040002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:14:20 log_id=00040002 msg_id=000000000106 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed health uptime-check1 from GUI
(172.20.120.47) "
```

### Related

- [00040001](#)
- [00040011](#)
- [19999496](#)

## 00040011

### Meaning

An administrator deleted a server availability monitor ("health check").

Field name	Description
<b>ID</b>	00040011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:14:30 log_id=00040011 msg_id=000000000107 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted health uptime-check1 from GUI
(172.20.120.47) "
```

### Related

- [00040002](#)
- [00040001](#)
- [19999496](#)

## 00040301

### Meaning

An administrator created a network service definition such as HTTP\_8080 or HTTPS4443.

Field name	Description
<b>ID</b>	00040301
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:23:14 log_id=00040301 msg_id=000000000138 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=succes smsg="User admin added custome service soap-service from GUI
(172.20.120.47) "
```

### Related

- [00040302](#)
- [00040311](#)

## 00040302

### Meaning

An administrator changed a network service definition.

Field name	Description
<b>ID</b>	00040302
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:23:18 log_id=00040302 msg_id=000000000139 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=succes smsg="User admin changed custom service soap-service from
GUI(172.20.120.47) "
```

### Related

- [00040301](#)
- [00040311](#)

## 00040311

### Meaning

An administrator deleted a network service definition.

Field name	Description
<b>ID</b>	00040311
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:23:34 log_id=00040311 msg_id=000000000140 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=succes smsg="User admin deleted custom service soap-service from GUI
(172.20.120.47) "
```

### Related

- [00040302](#)
- [00040301](#)



## 00040501

### Meaning

An administrator added a virtual server.

Field name	Description
<b>ID</b>	00040501
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=14:15:55 log_id=00040501 msg_id=000000055147 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added Virtual Server 1 from GUI(172.22.6.149) "
```

### Related

- [00040502](#)
- [00040511](#)

## 00040502

### Meaning

An administrator edited a virtual server.

Field name	Description
<b>ID</b>	00040502
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=14:16:22 log_id=00040502 msg_id=000000055149 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed Virtual Server FWB_Vserver from GUI(172.22.6.149) "
```

### Related

- [00040501](#)
- [00040511](#)

## 00040511

### Meaning

An administrator deleted a virtual server.

Field name	Description
<b>ID</b>	00040511
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=14:16:11 log_id=00040511 msg_id=000000055148 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted Virtual Server 1 from GUI(172.22.6.149) "
```

### Related

- [00040501](#)
- [00040502](#)

## 00040601

### Meaning

An administrator created an HTTP-layer route ("content route").

Field name	Description
<b>ID</b>	00040601
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:11:09 log_id=00040601 msg_id=0000000000091 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add
status=success msg="User admin added server-policy http-content-routing content-route1
from GUI(172.20.120.47) "
```

### Related

- [00040611](#)
- [00040623](#)
- [00030001](#)

## 00040611

### Meaning

An administrator deleted an HTTP-layer route ("content route").

Field name	Description
<b>ID</b>	00040611
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:11:45 log_id=00040611 msg_id=0000000000093 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted server-policy http-content-routing
content-route1 from GUI(172.20.120.47) "
```

### Related

- [00040601](#)
- [00040623](#)
- [00030001](#)

## 00040623

### Meaning

An administrator changed an HTTP-layer route ("content route").

Field name	Description
<b>ID</b>	00040623
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=14:24:08 log_id=00040623 msg_id=000000055157 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin changed server-policy http-content-routing FWB_ContentRouting1 list 2 from GUI (172.22.6.149) "
```

### Related

- [00040601](#)
- [00040611](#)
- [00030001](#)

## 00040751

### Meaning

An administrator uploaded a customized HTTP error web page.

Field name	Description
<b>ID</b>	00040751
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:18:58 log_id=00040751 msg_id=000000820249 device_
id=FVVM020000018475 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added server-policy error-page myerrorpage
from GUI(172.22.6.230)
```

### Related

- [00040752](#)
- [00040761](#)

## 00040752

### Meaning

An administrator changed the description for a customized HTTP error web page.

Field name	Description
<b>ID</b>	00040752
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:22:11 log_id=00040752 msg_id=000000000132 device_
id=FVVM00UNLICENSED timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit
status=success msg="User admin changed server-policy error-page custom-500 from GUI
(172.20.120.47) "
```

### Related

- [00040751](#)
- [00040761](#)



## 00040761

### Meaning

An administrator deleted a customized HTTP error web page.

Field name	Description
<b>ID</b>	00040761
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:22:21 log_id=00040761 msg_id=000000000133 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted server-policy error-page custom-500
from GUI(172.20.120.47)"
```

### Related

- [00040751](#)
- [00040752](#)

## 00040801

### Meaning

An administrator created a customized data type definition.

Field name	Description
<b>ID</b>	00040801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:36:11 log_id=00040801 msg_id=000000000156 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added server-policy pattern custom-data-type
data-type1 from GUI(172.20.120.47) "
```

### Related

- [00040802](#)
- [00040811](#)

## 00040802

### Meaning

An administrator changed a customized data type definition.

Field name	Description
<b>ID</b>	00040802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:36:14 log_id=00040802 msg_id=000000000157 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed server-policy pattern custom-data-
type data-type1 from GUI(172.20.120.47)"
```

### Related

- [00040801](#)
- [00040811](#)

## 00040811

### Meaning

An administrator deleted a customized data type definition.

Field name	Description
<b>ID</b>	00040811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:36:21 log_id=00040811 msg_id=000000000158 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted server-policy pattern custom-data-
type data-type1 from GUI(172.20.120.47)"
```

### Related

- [00040802](#)
- [00040801](#)

## 00040901

### Meaning

An administrator created a group of customized data type definitions.

Field name	Description
<b>ID</b>	00040901
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:37:29 log_id=00040901 msg_id=000000000160 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added server-policy pattern data-type-group
custom-data-type-group1 from GUI(172.20.120.47)"
```

### Related

- [00040902](#)
- [00040911](#)

## 00040902

### Meaning

An administrator changed a group of customized data type definitions.

Field name	Description
<b>ID</b>	00040902
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:37:39 log_id=00040902 msg_id=000000000161 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed server-policy pattern data-type-
group custom-data-type-group1 from GUI(172.20.120.47) "
```

### Related

- [00040901](#)
- [00040911](#)

## 00040911

### Meaning

An administrator deleted a group of customized data type definitions.

Field name	Description
<b>ID</b>	00040911
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:37:49 log_id=00040911 msg_id=000000000161 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted server-policy pattern data-type-
group custom-data-type-group1 from GUI(172.20.120.47) "
```

### Related

- [00040902](#)
- [00040901](#)

## 00041001

### Meaning

An administrator created a customized suspicious URL definition.

Field name	Description
<b>ID</b>	00041001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:35:29 log_id=00041001 msg_id=000000000152 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added custom-susp-url suspicious-url1 from
GUI(172.20.120.47) "
```

### Related

- [00041002](#)
- [00041011](#)



## 00041002

### Meaning

An administrator changed a customized suspicious URL definition.

Field name	Description
<b>ID</b>	00041002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:35:39 log_id=00041002 msg_id=000000000153 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed custom-susp-url suspicious-url1
from GUI(172.20.120.47) "
```

### Related

- [00041011](#)
- [00041001](#)

## 00041011

### Meaning

An administrator deleted a customized suspicious URL definition.

Field name	Description
<b>ID</b>	00041011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:35:49 log_id=00041011 msg_id=000000000153 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted custom-susp-url suspicious-url1 from
GUI(172.20.120.47) "
```

### Related

- [00041002](#)
- [00041001](#)

## 00041101

### Meaning

An administrator created a group of customized suspicious URL definitions ("policy").

Field name	Description
<b>ID</b>	00041101
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:35:44 log_id=00041101 msg_id=000000000153 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)
"type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added custom-susp-url-rule suspicious-urls-
all from GUI(172.20.120.47) "
```

### Related

- [00041102](#)
- [00041111](#)

## 00041102

### Meaning

An administrator changed a group of customized suspicious URL definitions.

Field name	Description
<b>ID</b>	00041102
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:35:45 log_id=00041102 msg_id=000000000154 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)
"type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed custom-susp-url-rule suspicious-
urls-all from GUI(172.20.120.47)"
```

### Related

- [00041101](#)
- [00041111](#)

## 00041111

### Meaning

An administrator deleted a group of customized suspicious URL definitions.

Field name	Description
<b>ID</b>	00041111
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:35:49 log_id=00041111 msg_id=000000000153 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted custom-susp-url suspicious-url1 from
GUI(172.20.120.47) "
```

### Related

- [00041101](#)
- [00041102](#)

## 00041201

### Meaning

An administrator created a customized suspicious URL definition ("rule").

Field name	Description
<b>ID</b>	00041201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:36:50 log_id=00041201 msg_id=000000000157 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added server-policy pattern suspicious-url-
rule custom-suspicious-urls from GUI(172.20.120.47) "
```

### Related

- [00041202](#)
- [00041211](#)

## 00041202

### Meaning

An administrator changed a customized suspicious URL definition.

Field name	Description
<b>ID</b>	00041202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:36:50 log_id=00041202 msg_id=000000000158 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed server-policy pattern suspicious-
url-rule custom-suspicious-urls from GUI(172.20.120.47) "
```

### Related

- [00041201](#)
- [00041211](#)

## 00041211

### Meaning

An administrator deleted a customized suspicious URL definition.

Field name	Description
<b>ID</b>	00041211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:36:50 log_id=00041211 msg_id=000000000158 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted server-policy pattern suspicious-
url-rule custom-suspicious-urls from GUI(172.20.120.47) "
```

### Related

- [00041201](#)
- [00041202](#)



## 00041302

### Meaning

An administrator disabled or enabled either:

- a predefined global white list object or
- a definition of a known search engine crawler.

Field name	Description
<b>ID</b>	00041302
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-01-08 time=17:39:20 log_id=00041302 msg_id=000000004887 device_id=FV-3KC3R09700002 vd="adom_auto" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed the Global White List"
```

```
date=2013-10-08 time=10:22:50 log_id=00041302 msg_id=000000000136 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )" type=event subtype="admin "pri=notification trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed the Global known Engines"
```

## 00041401

### Meaning

An administrator created an allowed/protected `Host` : definition.

Field name	Description
<b>ID</b>	00041401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:12:46 log_id=00041401 msg_id=000000000101 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added Protected Hostnames example_co_jp from
GUI(172.20.120.47) "
```

### Related

- [00041402](#)
- [00041411](#)

## 00041402

### Meaning

An administrator changed an allowed/protected `Host` : definition.

Field name	Description
<b>ID</b>	00041402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:12:52 log_id=00041402 msg_id=000000000102 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed Protected Hostnames example_com
from GUI(172.20.120.47) "
```

### Related

- [00041401](#)
- [00041411](#)

## 00041411

### Meaning

An administrator deleted an allowed/protected `Host` : definition.

Field name	Description
<b>ID</b>	00041411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-15 time=20:01:30 log_id=00041411 msg_id=000000000637 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted Protected Hostnames example_co_uk
from GUI(192.168.1.28) "
```

### Related

- [00041401](#)
- [00041402](#)

## 00041601

### Meaning

An administrator created an interpreter to locate parameters in a dynamic URL ("URL replacer") when using auto-learning.

### Field name

### Description

#### ID

00041601

(log\_id)

See [Log ID numbers on page 15](#).

### Examples

```
date=2013-10-08 time=10:34:46 log_id=00041601 msg_id=000000000148 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added server-policy custom-application url-
replace url-interpreter1 from GUI(172.20.120.47) "
```

### Related

- [00041602](#)
- [00041611](#)

## 00041602

### Meaning

An administrator changed a URL replacer.

Field name	Description
<b>ID</b>	00041602
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-15 time=20:31:58 log_id=00041602 msg_id=0000000000645 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed server-policy custom-application
url-replace url-interpret1 from GUI(192.168.1.28) "
```

### Related

- [00041601](#)
- [00041611](#)

## 00041611

### Meaning

An administrator deleted a URL replacer.

Field name	Description
<b>ID</b>	00041611
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:33:21 log_id=00041611 msg_id=000000000147 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted server-policy custom-application
url-replace url-interpreter1 from GUI(172.20.120.47) "
```

### Related

- [00041601](#)
- [00041602](#)

## 00041801

### Meaning

An administrator created a group of URL replacers ("application policy").

Field name	Description
<b>ID</b>	00041801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-15 time=20:32:24 log_id=00041801 msg_id=000000000647 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added server-policy custom-application
application-policy url-interpreter-group1 from GUI(192.168.1.28)"
```

### Related

- [00041802](#)
- [00041811](#)



## 00041802

### Meaning

An administrator changed a group of URL replacers ("application policy").

Field name	Description
<b>ID</b>	00041802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-15 time=20:32:29 log_id=00041802 msg_id=000000000648 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed server-policy custom-application
application-policy url-interpreter-group1 from GUI(192.168.1.28)"
```

### Related

- [00041801](#)
- [00041811](#)

## 00041811

### Meaning

An administrator deleted a group of URL replacers ("application policy").

Field name	Description
<b>ID</b>	00041811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-15 time=20:32:39 log_id=00041811 msg_id=000000000649 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted server-policy custom-application
application-policy url-interpreter-group1 from GUI(192.168.1.28)"
```

### Related

- [00041801](#)
- [00041802](#)

## 00043001

### Meaning

An administrator created a server policy.

Field name	Description
<b>ID</b>	00043001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:20:37 log_id=00043001 msg_id=000000000128 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added policy policy2 from GUI(172.20.120.47)
"
```

### Related

- [00043011](#)
- [00043002](#)

## 00043002

### Meaning

An administrator changed a server policy.

Field name	Description
<b>ID</b>	00043002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:20:04 log_id=00043002 msg_id=000000000125 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed policy policy1 from GUI
(172.20.120.47) "
```

### Related

- [00043001](#)
- [00043011](#)

## 00043011

### Meaning

An administrator deleted a server policy.

Field name	Description
<b>ID</b>	00043011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:20:49 log_id=00043011 msg_id=000000000130 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted policy policy2 from GUI
(172.20.120.47) "
```

### Related

- [00043001](#)
- [00043002](#)

## 00044001

### Meaning

An administrator added a site publishing policy rule.

Field name	Description
<b>ID</b>	00044001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:24:11 log_id=00044001 msg_id=000000179495 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=add status=success msg="User admin added site-
published-helper autotest.fwb.com from GUI(172.22.6.66) "
```

### Related

- [00044002](#)
- [00044011](#)
- [00044401](#)
- [00044411](#)

## 00044002

### Meaning

An administrator edited a site publishing policy rule.

Field name	Description
<b>ID</b>	00044002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:30:16 log_id=00044002 msg_id=000000179501 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=edit status=success msg="User admin changed site-
published-helper autotest1.fwb.com from GUI(172.22.6.66) "
```

### Related

- [00044001](#)
- [00044011](#)
- [00044401](#)
- [00044411](#)

## 00044011

### Meaning

An administrator deleted a site publishing policy rule.

Field name	Description
<b>ID</b>	00044011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:31:41 log_id=00044011 msg_id=000000179502 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=del status=success msg="User admin deleted site-
published-helper autotest1.fwb.com from GUI(172.22.6.66)"
```

### Related

- [00044001](#)
- [00044002](#)
- [00044401](#)
- [00044411](#)



## 00044401

### Meaning

An administrator added a site publishing policy.

Field name	Description
<b>ID</b>	00044401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:32:28 log_id=00044401 msg_id=000000179503 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=add status=success msg="User admin added site-
published-helper-policy dd from GUI(172.22.6.66)"
```

### Related

- [00044411](#)
- [00044001](#)
- [00044002](#)
- [00044011](#)

## 00044411

### Meaning

An administrator deleted a site publishing policy.

Field name	Description
<b>ID</b>	00044411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:38:07 log_id=00044411 msg_id=000000179507 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=del status=success msg="User admin deleted site-
published-helper-policy dd from GUI(172.22.6.66)"
```

### Related

- [00044401](#)
- [00044001](#)
- [00044002](#)
- [00044011](#)

## 00044501

### Meaning

An administrator added a custom global whitelist item.

Field name	Description
<b>ID</b>	00044501
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=15:03:01 log_id=00044501 msg_id=000000055170 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-global-whilte-list-group 1 from GUI(172.22.6.149) "
```

### Related

- [00044502](#)
- [00044511](#)

## 00044502

### Meaning

An administrator edited a custom global whitelist item.

Field name	Description
<b>ID</b>	00044502
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=15:03:26 log_id=00044502 msg_id=000000055171 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-global-whilte-list-group 1 from GUI(172.22.6.149) "
```

### Related

- [00044501](#)
- [00044511](#)

## 00044511

### Meaning

An administrator deleted a custom global whitelist item.

Field name	Description
<b>ID</b>	00044511
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=15:03:40 log_id=00044511 msg_id=000000055172 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-global-whilte-list-group 1 from GUI(172.22.6.149) "
```

### Related

- [00044501](#)
- [00044502](#)

## 00046001

### Meaning

An administrator created a session persistence configuration.

Field name	Description
<b>ID</b>	00046001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-03 time=10:47:27 log_id=00046001 msg_id=000000003145 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add
status=success msg="User admin added persistence-policy persistent_ip from GUI
(172.20.120.61) "
```

### Related

- [00046002](#)
- [00046011](#)

## 00046002

### Meaning

An administrator edited a session persistence configuration.

Field name	Description
<b>ID</b>	00046002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-03 time=10:56:36 log_id=00046002 msg_id=000000003146 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit
status=success msg="User admin changed persistence-policy persistent_ip from GUI
(172.20.120.61) "
```

### Related

- [00046001](#)
- [00046011](#)

## 00046011

### Meaning

An administrator deleted a session persistence configuration.

Field name	Description
<b>ID</b>	00046011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-03 time=10:56:56 log_id=00046011 msg_id=000000003147 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del
status=success msg="User admin deleted persistence-policy persistent_ip from GUI
(172.20.120.61) "
```

### Related

- [00046001](#)
- [00046002](#)



## 00050001

### Meaning

An administrator created a compression exemption.

Field name	Description
<b>ID</b>	00050001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:55:44 log_id=00050001 msg_id=000000000240 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added exclude-url gzip-exempt1 from GUI
(172.20.120.47) "
```

### Related

- [00050002](#)
- [00050011](#)

## 00050002

### Meaning

An administrator changed a compression exemption.

Field name	Description
<b>ID</b>	00050002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:55:55 log_id=00050002 msg_id=000000000241 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed exclude-url gzip-exempt1 from GUI
(172.20.120.47) "
```

### Related

- [00050001](#)
- [00050011](#)

## 00050011

### Meaning

An administrator deleted a compression exemption.

Field name	Description
<b>ID</b>	00050011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:56:55 log_id=00050011 msg_id=000000000242 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted exclude-url gzip-exempt1 from GUI
(172.20.120.47) "
```

### Related

- [00050001](#)
- [00050002](#)

## 00050201

### Meaning

An administrator created a decompressor.

Field name	Description
<b>ID</b>	00050201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:56:11 log_id=00050201 msg_id=000000000243 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added file-uncompress-rule decompressor1
from GUI(172.20.120.47) "
```

### Related

- [00050202](#)
- [00050211](#)

## 00050202

### Meaning

An administrator changed a decompressor.

Field name	Description
<b>ID</b>	00050202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:56:23 log_id=00050202 msg_id=000000000244 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed file-uncompress-rule decompressor1
from GUI(172.20.120.47) "
```

### Related

- [00050201](#)
- [00050211](#)

## 00050211

### Meaning

An administrator deleted a decompressor.

Field name	Description
<b>ID</b>	00050211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:56:43 log_id=00050211 msg_id=000000000245 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin dleted file-uncompress-rule decompressor1
from GUI(172.20.120.47) "
```

### Related

- [00050201](#)
- [00050202](#)

## 00050401

### Meaning

An administrator created a compressor.

Field name	Description
<b>ID</b>	00050401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:56:34 log_id=00050401 msg_id=000000000245 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added file-compress-rule compressor1 from
GUI(172.20.120.47) "
```

### Related

- [00050402](#)
- [00050411](#)

## 00050402

### Meaning

An administrator changed a compressor.

Field name	Description
<b>ID</b>	00050402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:56:46 log_id=00050402 msg_id=000000000246 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed file-compress-rule compressor1 from
GUI(172.20.120.47) "
```

### Related

- [00050401](#)
- [00050411](#)



## 00050411

### Meaning

An administrator deleted a compressor.

Field name	Description
<b>ID</b>	00050411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:56:56 log_id=00050411 msg_id=000000000247 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted file-compress-rule compressor1 from
GUI(172.20.120.47) "
```

### Related

- [00050401](#)
- [00050402](#)

## 00051001

### Meaning

An administrator created an HTTP flood prevention rule.

Field name	Description
<b>ID</b>	00051001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:40:19 log_id=00051001 msg_id=000000000175 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added http-request-flood-prevention-rule
http-flood-ip1 from GUI(172.20.120.47) "
```

### Related

- [00051002](#)
- [00051011](#)

## 00051002

### Meaning

An administrator changed an HTTP flood prevention rule.

Field name	Description
<b>ID</b>	00051002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:36:04 log_id=00051002 msg_id=000000000418 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed http-request-flood-prevention-rule
http-flood-ip1 from GUI(172.20.120.47) "
```

### Related

- [00051001](#)
- [00051011](#)

## 00051011

### Meaning

An administrator deleted an HTTP flood prevention rule.

Field name	Description
<b>ID</b>	00051011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:36:24 log_id=00051011 msg_id=000000000419 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted http-request-flood-prevention-rule
http-flood-ip1 from GUI(172.20.120.47) "
```

### Related

- [00051001](#)
- [00051002](#)

## 00051201

### Meaning

An administrator created a malicious IPs rule.

Field name	Description
<b>ID</b>	00051201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:40:35 log_id=00051201 msg_id=000000000176 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added http-connection-flood-check-rule dos-
ip1 from GUI(172.20.120.47) "
```

### Related

- [00051202](#)
- [00051211](#)

## 00051202

### Meaning

An administrator changed a malicious IPs rule.

Field name	Description
<b>ID</b>	00051202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:36:13 log_id=00051202 msg_id=0000000000419 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed http-connection-flood-check-rule
dos-ip1 from GUI(172.20.120.47) "
```

### Relate

- [00051201](#)
- [00051211](#)

## 00051211

### Meaning

An administrator deleted a malicious IPs rule.

Field name	Description
<b>ID</b>	00051211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:36:23 log_id=00051211 msg_id=000000000420 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted http-connection-flood-check-rule
dos-ip1 from GUI(172.20.120.47) "
```

### Related

- [00051201](#)
- [00051202](#)

## 00051401

### Meaning

An administrator created a HTTP access limit rule.

Field name	Description
<b>ID</b>	00051401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:40:35 log_id=00051401 msg_id=000000000176 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added layer4-access-limit-rule dos-ip1 from
GUI (172.20.120.47) "
```

### Related

- [00051402](#)
- [00051411](#)



## 00051402

### Meaning

An administrator changed a HTTP access limit rule.

Field name	Description
<b>ID</b>	00051402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:36:13 log_id=00051402 msg_id=000000000419 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed layer4-access-limit-rule dos-ip1
from GUI(172.20.120.47) "
```

### Related

- [00051401](#)
- [00051411](#)

## 00051411

### Meaning

An administrator deleted a HTTP access limit rule.

Field name	Description
<b>ID</b>	00051411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:36:23 log_id=00051411 msg_id=000000000420 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted layer4-access-limit-rule dos-ip1
from GUI(172.20.120.47) "
```

### Related

- [00051401](#)
- [00051402](#)

## 00051601

### Meaning

An administrator created a TCP flood prevention rule.

Field name	Description
<b>ID</b>	00051601
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:41:36 log_id=00051601 msg_id=000000000178 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added waf-layer4-connection-flood-check-rule
tcp-flood-preventer1 from GUI(172.20.120.47) "
```

### Related

- [00051602](#)
- [00051611](#)

## 00051602

### Meaning

An administrator changed a TCP flood prevention rule.

Field name	Description
<b>ID</b>	00051602
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:35:51 log_id=00051602 msg_id=000000000417 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed waf-layer4-connection-flood-check-
rule tcp-flood-preventer1 from GUI(172.20.120.47) "
```

### Related

- [00051601](#)
- [00051611](#)

## 00051611

### Meaning

An administrator deleted a TCP flood prevention rule.

Field name	Description
<b>ID</b>	00051611
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:35:59 log_id=00051611 msg_id=000000000418 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin changed waf-layer4-connection-flood-check-
rule tcp-flood-preventer1 from GUI(172.20.120.47) "
```

### Related

- [00051601](#)
- [00051602](#)

## 00051801

### Meaning

An administrator created a DoS protection policy.

Field name	Description
<b>ID</b>	00051801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:38:42 log_id=00051801 msg_id=000000000173 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added DoS protection policy dos-protection1
from GUI(172.20.120.47) "
```

### Related

- [00051802](#)
- [00051811](#)

## 00051802

### Meaning

An administrator changed a DoS protection policy.

Field name	Description
<b>ID</b>	00051802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:41:46 log_id=00051802 msg_id=000000000179 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed DoS protection policy dos-
protection1 from GUI(172.20.120.47) "
```

### Related

- [00051801](#)
- [00051811](#)

## 00051811

### Meaning

An administrator deleted a DoS protection policy.

Field name	Description
<b>ID</b>	00051811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:41:56 log_id=00051811 msg_id=000000000180 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted DoS protection policy dos-
protection1 from GUI(172.20.120.47) "
```

### Related

- [00051801](#)
- [00051802](#)



## 00052201

### Meaning

An administrator created a client IP white list or black list.

Field name	Description
<b>ID</b>	00052201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-11 time=09:57:02 log_id=00052201 msg_id=000000000460 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added waf ip-list blacklist from GUI
(172.20.120.47) "
```

### Related

- [00052202](#)
- [00052211](#)

## 00052202

### Meaning

An administrator changed a client IP white list or black list.

Field name	Description
<b>ID</b>	00052202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-11 time=09:57:12 log_id=00052202 msg_id=000000000461 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed waf ip-list blacklist from GUI
(172.20.120.47) "
```

### Related

- [00052201](#)
- [00052211](#)

## 00052211

### Meaning

An administrator deleted a client IP white list or black list.

Field name	Description
<b>ID</b>	00052211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-11 time=09:57:22 log_id=00052211 msg_id=000000000462 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted waf ip-list blacklist from GUI
(172.20.120.47) "
```

### Related

- [00052201](#)
- [00052202](#)

## 00052401

### Meaning

An administrator created a user authentication rule.

Field name	Description
<b>ID</b>	00040002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:14:20 log_id=00040002 msg_id=000000000106 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed health uptime-check1 from GUI
(172.20.120.47) "
```

### Related

- [00052402](#)
- [00052411](#)

## 00052402

### Meaning

An administrator changed a user authentication rule.

Field name	Description
<b>ID</b>	00052402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:57:33 log_id=00052402 msg_id=000000000255 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed http-authen-rule user-auth-realms1
from GUI(172.20.120.47) "
```

### Related

- [00052401](#)
- [00052411](#)

## 00052411

### Meaning

An administrator deleted a user authentication rule.

Field name	Description
<b>ID</b>	00052411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-09 time=16:15:22 log_id=00052411 msg_id=000000000316 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted http-authen-rule user-auth-realms1
from GUI(172.20.120.47) "
```

### Related

- [00052401](#)
- [00052402](#)

## 00052601

### Meaning

An administrator created a user authentication policy.

Field name	Description
<b>ID</b>	00052601
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:57:59 log_id=00052601 msg_id=000000000257 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added http-authen-policy user-auth-policy1
from GUI(172.20.120.47) "
```

### Related

- [00052602](#)
- [00052611](#)

## 00052602

### Meaning

An administrator changed a user authentication policy.

Field name	Description
<b>ID</b>	00052602
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:58:02 log_id=00052602 msg_id=000000000258 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed http-authen-policy user-auth-
policy1 from GUI(172.20.120.47) "
```

### Related

- [00052601](#)
- [00052611](#)



## 00052611

### Meaning

An administrator deleted a user authentication policy.

Field name	Description
<b>ID</b>	00052611
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-09 time=16:15:17 log_id=00052611 msg_id=000000000315 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted http-authen-policy user-auth-
connections-temp from GUI(172.20.120.47) "
```

### Related

- [00052601](#)
- [00052602](#)

## 00053201

### Meaning

An administrator added an input rule for HTTP requests.

Field name	Description
<b>ID</b>	00053201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:50:46 log_id=00053201 msg_id=000000734635 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added input-rule dddd from GUI(172.22.6.237) "
```

### Related

- [00053202](#)
- [00053211](#)

## 00053202

### Meaning

An administrator edited an input rule for HTTP requests.

Field name	Description
<b>ID</b>	00053202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:54:39 log_id=00053202 msg_id=000000734636 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed input-rule dddd from GUI(172.22.6.237) "
```

### Related

- [00053201](#)
- [00053211](#)

## 00053211

### Meaning

An administrator deleted an input rule for HTTP requests.

Field name	Description
<b>ID</b>	00053211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:56:42 log_id=00053211 msg_id=000000734637 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted input-rule dddd from GUI(172.22.6.237) "
```

### Related

- [00053201](#)
- [00053202](#)

## 00053701

### Meaning

An administrator added a parameter validation rule.

Field name	Description
<b>ID</b>	00053701
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:41:56 log_id=00053701 msg_id=000000734632 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added parameter-validation-rule 123 from GUI (172.22.6.237) "
```

### Related

- [00053711](#)

## 00053711

### Meaning

An administrator deleted a parameter validation rule.

Field name	Description
<b>ID</b>	00053711
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:49:47 log_id=00053711 msg_id=000000734634 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted parameter-validation-rule 123 from GUI (172.22.6.237) "
```

### Related

- [00053701](#)

## 00053901

### Meaning

An administrator created a hidden input rule.

Field name	Description
<b>ID</b>	00053901
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:51:19 log_id=00053901 msg_id=000000000218 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added hidden-fields-rule hidden-input-rule1
from GUI(172.20.120.47) "
```

### Related

- [00053902](#)
- [00053911](#)

## 00053902

### Meaning

An administrator changed a hidden input rule.

Field name	Description
<b>ID</b>	00053902
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:51:25 log_id=00053902 msg_id=000000000219 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed hidden-fields-rule hidden-input-
rule1 from GUI(172.20.120.47) "
```

### Related

- [00053901](#)
- [00053911](#)



## 00053911

### Meaning

An administrator deleted a hidden input rule.

Field name	Description
<b>ID</b>	00053911
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:51:35 log_id=00053911 msg_id=000000000220 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted hidden-fields-rule hidden-input-
rule1 from GUI(172.20.120.47) "
```

### Related

- [00053901](#)
- [00053902](#)

## 00054401

### Meaning

An administrator created a hidden input policy.

Field name	Description
<b>ID</b>	00054401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:52:11 log_id=00054401 msg_id=000000000222 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added hidden-fields-protection hidden-input-
policy1 from GUI(172.20.120.47) "
```

### Related

- [00054402](#)
- [00054411](#)

## 00054402

### Meaning

An administrator changed a hidden input policy.

Field name	Description
<b>ID</b>	00054402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:52:16 log_id=00054402 msg_id=000000000223 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed hidden-fields-protection hidden-
input-policy1 from GUI(172.20.120.47) "
```

### Related

- [00054401](#)
- [00054411](#)

## 00054411

### Meaning

An administrator deleted a hidden input policy.

Field name	Description
<b>ID</b>	00054411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:52:26 log_id=00054411 msg_id=000000000224 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted hidden-fields-protection hidden-
input-policy1 from GUI(172.20.120.47) "
```

### Related

- [00054401](#)
- [00054402](#)

## 00054601

### Meaning

An administrator created a page order rule.

Field name	Description
<b>ID</b>	00054601
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:44:40 log_id=00054601 msg_id=000000000191 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added page-access-rule page-order1 from GUI
(172.20.120.47) "
```

### Related

- [00054602](#)
- [00054611](#)

## 00054602

### Meaning

An administrator changed a page order rule.

Field name	Description
<b>ID</b>	00054602
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:44:49 log_id=00054602 msg_id=000000000192 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed page-access-rule page-order1 from
GUI(172.20.120.47) "
```

### Related

- [00054601](#)
- [00054611](#)

## 00054611

### Meaning

An administrator deleted a page order rule.

Field name	Description
<b>ID</b>	00054611
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:44:49 log_id=00054611 msg_id=000000000193 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted page-access-rule page-order1 from
GUI(172.20.120.47) "
```

### Related

- [00054601](#)
- [00054602](#)

## 00054801

### Meaning

An administrator created a rewrite/redirect rule.

Field name	Description
<b>ID</b>	00054801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=11:07:40 log_id=00054801 msg_id=000000000263 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added url-rewrite-rule http-to-https-
redirect from GUI(172.20.120.47) "
```

### Related

- [00054802](#)
- [00054811](#)



## 00054802

### Meaning

An administrator changed a rewrite/redirect rule.

Field name	Description
<b>ID</b>	00054802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=11:07:55 log_id=00054802 msg_id=000000000264 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed url-rewrite-rule http-to-https-
redirect from GUI(172.20.120.47) "
```

### Related

- [00054801](#)
- [00054811](#)

## 00054811

### Meaning

An administrator deleted a rewrite/redirect rule.

Field name	Description
<b>ID</b>	00054811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=11:08:55 log_id=00054811 msg_id=000000000265 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted url-rewrite-rule http-to-https-
redirect from GUI(172.20.120.47) "
```

### Related

- [00054801](#)
- [00054802](#)

## 00055301

### Meaning

An administrator created a rewrite/redirect policy.

Field name	Description
<b>ID</b>	00055301
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=11:09:10 log_id=00055301 msg_id=000000000268 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added url-rewrite-policy request-rewrites1
from GUI(172.20.120.47) "
```

### Related

- [00055302](#)
- [00055311](#)

## 00055302

### Meaning

An administrator changed a rewrite/redirect policy.

Field name	Description
<b>ID</b>	00055302
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=11:09:14 log_id=00055302 msg_id=000000000269 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed url-rewrite-policy request-
rewrites1 from GUI(172.20.120.47) "
```

### Related

- [00055301](#)
- [00055311](#)

## 00055311

### Meaning

An administrator deleted a rewrite/redirect policy.

Field name	Description
<b>ID</b>	00055311
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=11:09:34 log_id=00055311 msg_id=000000000270 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted url-rewrite-policy request-rewrites1
from GUI(172.20.120.47) "
```

### Related

- [00055301](#)
- [00055302](#)

## 00055501

### Meaning

An administrator created an allowed HTTP method exception.

Field name	Description
<b>ID</b>	00055501
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:42:10 log_id=00055501 msg_id=000000000180 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added allow-method-exceptions method-exempt1
from GUI(172.20.120.47) "
```

### Related

- [00055502](#)
- [00055511](#)

## 00055502

### Meaning

An administrator changed an allowed HTTP method exception.

Field name	Description
<b>ID</b>	00055502
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:42:33 log_id=00055502 msg_id=000000000181 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed allow-method-exceptions method-
exempt1 from GUI(172.20.120.47) "
```

### Related

- [00055501](#)
- [00055511](#)

## 00055511

### Meaning

An administrator deleted an allowed HTTP method exception.

Field name	Description
<b>ID</b>	00055511
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:42:43 log_id=00055511 msg_id=000000000182 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted allow-method-exceptions method-
exempt1 from GUI(172.20.120.47) "
```

### Related

- [00055501](#)
- [00055502](#)



## 00055701

### Meaning

An administrator created an allowed HTTP method.

Field name	Description
<b>ID</b>	00055701
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:43:04 log_id=00055701 msg_id=000000000183 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added allow-method-policy allowed-methods1
from GUI(172.20.120.47) "
```

### Related

- [00055702](#)
- [00055711](#)

## 00055702

### Meaning

An administrator changed an allowed HTTP method.

Field name	Description
<b>ID</b>	00055702
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:43:14 log_id=00055702 msg_id=000000000184 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed allow-method-policy allowed-
methods1 from GUI(172.20.120.47) "
```

### Related

- [00055701](#)
- [00055711](#)

## 00055711

### Meaning

An administrator deleted an allowed HTTP method.

Field name	Description
<b>ID</b>	00055711
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:43:24 log_id=00055711 msg_id=000000000185 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted allow-method-policy allowed-methods1
from GUI(172.20.120.47) "
```

### Related

- [00055701](#)
- [00055702](#)

## 00055901

### Meaning

An administrator created an access control rule.

Field name	Description
<b>ID</b>	00055901
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:46:02 log_id=00055901 msg_id=000000000196 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added url-access-rule access-controll from
GUI(172.20.120.47) "
```

### Related

- [00055902](#)
- [00055911](#)

## 00055902

### Meaning

An administrator changed an access control rule.

Field name	Description
<b>ID</b>	00055902
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:46:12 log_id=00055902 msg_id=000000000197 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed url-access-rule access-controll
from GUI(172.20.120.47) "
```

### Related

- [00055901](#)
- [00055911](#)

## 00055911

### Meaning

An administrator deleted an access control rule.

Field name	Description
<b>ID</b>	00055911
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:46:22 log_id=00055911 msg_id=000000000198 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted url-access-rule access-controll from
GUI(172.20.120.47) "
```

### Related

- [00055901](#)
- [00055902](#)

## 00056401

### Meaning

An administrator created an access control policy.

Field name	Description
<b>ID</b>	00056401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:46:42 log_id=00056401 msg_id=000000000199 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added url-access-policy access-control-
group1 from GUI(172.20.120.47) "
```

### Related

- [00056402](#)
- [00056411](#)

## 00056402

### Meaning

An administrator changed an access control policy.

Field name	Description
<b>ID</b>	00056402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:47:04 log_id=00056402 msg_id=000000000202 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed url-access-policy access-control-
group1 from GUI(172.20.120.47) "
```

### Related

- [00056401](#)
- [00056411](#)



## 00056411

### Meaning

An administrator deleted an access control policy.

Field name	Description
<b>ID</b>	00056411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:47:14 log_id=00056411 msg_id=000000000203 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted url-access-policy access-control-
group1 from GUI(172.20.120.47) "
```

### Related

- [00056401](#)
- [00056402](#)

## 00056601

### Meaning

An administrator created an HTTP constraint.

Field name	Description
<b>ID</b>	00056601
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:48:21 log_id=00056601 msg_id=000000000207 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added http-protocol-parameter-restriction
http-contraints1 from GUI(172.20.120.47)"
```

### Related

- [00056602](#)
- [00056611](#)

## 00056602

### Meaning

An administrator changed an HTTP constraint.

Field name	Description
<b>ID</b>	00056602
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-11 time=10:17:50 log_id=00056602 msg_id=000000000482 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed http-protocol-parameter-restriction
http-contraints1 from GUI(172.20.120.47)"
```

### Related

- [00056601](#)
- [00056611](#)

## 00056611

### Meaning

An administrator deleted an HTTP constraint.

Field name	Description
<b>ID</b>	00056611
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-11 time=10:17:59log_id=00056611 msg_id=000000000483 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted http-protocol-parameter-restriction
http-contraints1 from GUI(172.20.120.47)"
```

### Related

- [00056601](#)
- [00056602](#)

## 00058601

### Meaning

An administrator created an HTTP constraint exemption.

Field name	Description
<b>ID</b>	00058601
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:47:28 log_id=00058601 msg_id=000000000204 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added http-constraints-exception http-
constraints-exempt1 from GUI(172.20.120.47) "
```

### Related

- [00058602](#)
- [00058611](#)

## 00058602

### Meaning

An administrator changed an HTTP constraint exemption.

Field name	Description
<b>ID</b>	00058602
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:47:51 log_id=00058602 msg_id=000000000205 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed http-constraints-exception http-
constraints-exempt1 from GUI(172.20.120.47) "
```

### Related

- [00058601](#)
- [00058611](#)

## 00058611

### Meaning

An administrator deleted an HTTP constraint exemption.

Field name	Description
<b>ID</b>	00058611
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:48:51 log_id=00058611 msg_id=000000000206 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted http-constraints-exception http-
constraints-exempt1 from GUI(172.20.120.47) "
```

### Related

- [00058601](#)
- [00058602](#)

## 00059801

### Meaning

An administrator created a custom signature.

Field name	Description
<b>ID</b>	00059801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:54:06 log_id=00059801 msg_id=000000000232 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added custom-protection-rule custom-
signature1 from GUI(172.20.120.47) "
```

### Related

- [00059802](#)
- [00059811](#)



## 00059802

### Meaning

An administrator changed a custom signature.

Field name	Description
<b>ID</b>	00059802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:54:22 log_id=00059802 msg_id=000000000233 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed custom-protection-rule custom-
signature1 from GUI(172.20.120.47) "
```

### Related

- [00059801](#)
- [00059811](#)

## 00059811

### Meaning

An administrator deleted a custom signature.

Field name	Description
<b>ID</b>	00059811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:55:25 log_id=00059811 msg_id=000000000239 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted custom-protection-rule custom-
signature2 from GUI(172.20.120.47) "
```

### Related

- [00059801](#)
- [00059802](#)

## 00060001

### Meaning

An administrator created a group of custom signatures.

Field name	Description
<b>ID</b>	00060001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:54:46 log_id=00060001 msg_id=000000000235 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added custom-protection-group custom-
signatures1 from GUI(172.20.120.47) "
```

### Related

- [00060002](#)
- [00060011](#)

## 00060002

### Meaning

An administrator changed a group of custom signatures.

Field name	Description
<b>ID</b>	00060002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:54:51 log_id=00060002 msg_id=000000000236 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed custom-protection-group custom-
signatures1 from GUI(172.20.120.47) "
```

### Related

- [00060001](#)
- [00060011](#)

## 00060011

### Meaning

An administrator deleted a group of custom signatures.

Field name	Description
<b>ID</b>	00060011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:55:51 log_id=00060011 msg_id=000000000237 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=delstatus=success msg="User admin deleted custom-protection-group custom-
signatures1 from GUI(172.20.120.47) "
```

### Related

- [00060001](#)
- [00060002](#)

## 00060201

### Meaning

An administrator created an attack signatures rule.

Field name	Description
<b>ID</b>	00060201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=21:58:28 log_id=00060201 msg_id=000000000762 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added signature attack-signatures2 from GUI
(192.168.1.28) "
```

### Related

- [00060202](#)
- [00060211](#)

## 00060202

### Meaning

An administrator changed an attack signatures rule.

Field name	Description
<b>ID</b>	00060202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=21:47:39 log_id=00060202 msg_id=000000000759 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed signature attack-signatures1 from
GUI(192.168.1.28)"
```

### Related

- [00060201](#)
- [00060211](#)

## 00060211

### Meaning

An administrator deleted an attack signatures rule.

Field name	Description
<b>ID</b>	00060211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=21:58:46 log_id=00060211 msg_id=000000000763 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted signature attack-signatures2 from
GUI(192.168.1.28)"
```

### Related

[00060201](#) .....  
[00060202](#) .....



## 00061201

### Meaning

An administrator created an X-Forwarded-For : rule.

Field name	Description
<b>ID</b>	00061201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=22:04:30 log_id=00061201 msg_id=000000000764 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added x-forwarded-for xff1 from GUI
(192.168.1.28) "
```

### Related

- [00061202](#)
- [00061211](#)

## 00061202

### Meaning

An administrator changed an X-Forwarded-For : rule.

Field name	Description
<b>ID</b>	00061202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=22:04:35 log_id=00061202 msg_id=000000000765 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed x-forwarded-for xff1 from GUI
(192.168.1.28) "
```

### Related

- [00061201](#)
- [00061211](#)

## 00061211

### Meaning

An administrator deleted an X-Forwarded-For : rule.

Field name	Description
<b>ID</b>	00061211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=22:04:44 log_id=00061211 msg_id=000000000766 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted x-forwarded-for xff1 from GUI
(192.168.1.28) "
```

### Related

- [00061201](#)
- [00061202](#)

## 00061401

### Meaning

An administrator created a session initiation rule ("start page rule").

Field name	Description
<b>ID</b>	00061401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:43:33 log_id=00061401 msg_id=000000000184 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added start-pages session-init-page1 from
GUI(172.20.120.47) "
```

### Related

- [00061402](#)
- [00061411](#)

## 00061402

### Meaning

An administrator changed a session initiation rule ("start page rule").

Field name	Description
<b>ID</b>	00061402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:43:46 log_id=00061402 msg_id=000000000185 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed start-pages session-init-page1 from
GUI(172.20.120.47) "
```

### Related

- [00061401](#)
- [00061411](#)

## 00061411

### Meaning

An administrator deleted a session initiation rule ("start page rule").

Field name	Description
<b>ID</b>	00061411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:43:56 log_id=00061411 msg_id=000000000186 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted start-pages session-init-page1 from
GUI(172.20.120.47) "
```

### Related

- [00061401](#)
- [00061402](#)

## 00061801

### Meaning

An administrator has added a brute force login attack profile.

Field name	Description
<b>ID</b>	00061801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=10:38:38 log_id=00061801 msg_id=000000055127 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-brute-force-login dwg from GUI(172.22.6.149) "
```

### Related

- [00061802](#)
- [00061811](#)

## 00061802

### Meaning

An administrator edited a brute force login attack profile.

Field name	Description
<b>ID</b>	00061802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=11:15:21 log_id=00061802 msg_id=000000055128 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-brute-force-login dwg from GUI(172.22.6.149) "
```

### Related

- [00061801](#)
- [00061811](#)



## 00061811

### Meaning

An administrator has edited a brute force login attack profile.

Field name	Description
<b>ID</b>	00061811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=11:15:47 log_id=00061811 msg_id=000000055129 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf-brute-force-login dwg from GUI(172.22.6.149) "
```

### Related

- [00061801](#)
- [00061802](#)

## 00062001

### Meaning

An administrator created an upload restriction rule.

Field name	Description
<b>ID</b>	00062001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:49:10 log_id=00062001 msg_id=000000000208 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added file-upload-restriction-rule video-
uploads-limit1 from GUI(172.20.120.47) "
```

### Related

- [00062002](#)
- [00062011](#)

## 00062002

### Meaning

An administrator changed an upload restriction rule.

Field name	Description
<b>ID</b>	00062002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:49:49 log_id=00062002 msg_id=000000000209 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed file-upload-restriction-rule video-
uploads-limit1 from GUI(172.20.120.47) "
```

### Related

- [00062001](#)
- [00062011](#)

## 00062011

### Meaning

An administrator deleted an upload restriction rule.

Field name	Description
<b>ID</b>	00062011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:49:59 log_id=00062011 msg_id=000000000210 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted file-upload-restriction-rule video-
uploads-limit1 from GUI(172.20.120.47) "
```

### Related

- [00062001](#)
- [00062002](#)

## 00062201

### Meaning

An administrator created an upload restriction policy.

Field name	Description
<b>ID</b>	00062201
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=22:27:13 log_id=00062201 msg_id=000000000770 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added waf-file-upload-restriction-policy
all-file-uploads1 from GUI(192.168.1.28)"
```

### Related

- [00062202](#)
- [00062011](#)

## 00062202

### Meaning

An administrator changed an upload restriction policy.

Field name	Description
<b>ID</b>	00062202
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=22:27:24 log_id=00062202 msg_id=000000000772 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed waf-file-upload-restriction-policy
all-file-uploads1 from GUI(192.168.1.28)"
```

### Related

- [00062201](#)
- [00062211](#)

## 00062211

### Meaning

An administrator deleted an upload restriction policy.

Field name	Description
<b>ID</b>	00062211
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=22:27:32 log_id=00062211 msg_id=000000000773 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted waf-file-upload-restriction-policy
file-uploads from GUI(192.168.1.28) "
```

### Related

- [00062201](#)
- [00062202](#)

## 00062401

### Meaning

An administrator created an inline protection profile.

Field name	Description
<b>ID</b>	00062401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:09:59 log_id=00062401 msg_id=0000000000088 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added inline-protection inline-protection-
profile1 from GUI(172.20.120.47) "
```

### Related

- [00062402](#)
- [00062411](#)



## 00062402

### Meaning

An administrator changed an inline protection profile.

Field name	Description
<b>ID</b>	00062402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-10 time=00:32:06 log_id=00062402 msg_id=000000000377 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed inline-protection inline-
protection-profile1 from GUI(172.20.120.47) "
```

### Related

- [00062401](#)
- [00062411](#)

## 00062411

### Meaning

An administrator deleted an inline protection profile.

Field name	Description
<b>ID</b>	00062411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:18:34 log_id=00062411 msg_id=000000000118 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted inline-protection temp from GUI
(172.20.120.47) "
```

### Related

- [00062401](#)
- [00062402](#)

## 00063401

### Meaning

An administrator created an offline protection profile.

Field name	Description
<b>ID</b>	00063401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:18:44 log_id=00063401 msg_id=000000000119 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added offline-protection temp from GUI
(172.20.120.47) "
```

### Related

- [00063402](#)
- [00063411](#)

## 00063402

### Meaning

An administrator changed an offline protection profile.

Field name	Description
<b>ID</b>	00063402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:18:49 log_id=00063402 msg_id=000000000120 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed offline-protection temp from GUI
(172.20.120.47) "
```

### Related

- [00063401](#)
- [00063411](#)

## 00063411

### Meaning

An administrator deleted an offline protection profile.

Field name	Description
<b>ID</b>	00063411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:18:53 log_id=00063411 msg_id=000000000121 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted offline-protection temp from GUI
(172.20.120.47) "
```

### Related

- [00063401](#)
- [00063402](#)

## 00064401

### Meaning

An administrator created an auto-learning profile.

Field name	Description
<b>ID</b>	00064401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:37:50 log_id=00064401 msg_id=000000000166 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added autolearning-profile auto-learning1
from GUI(172.20.120.47) "
```

### Related

- [00064402](#)
- [00064411](#)

## 00064402

### Meaning

An administrator changed an auto-learning profile.

Field name	Description
<b>ID</b>	00064402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-15 time=20:31:30 log_id=00064402 msg_id=0000000000643 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed autolearning-profile auto-learning2
from GUI(192.168.1.28) "
```

### Related

- [00064401](#)
- [00064411](#)

## 00064411

### Meaning

An administrator deleted an auto-learning profile.

Field name	Description
<b>ID</b>	00064411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-15 time=20:31:37 log_id=00064411 msg_id=0000000000644 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted autolearning-profile auto-learning2
from GUI(192.168.1.28) "
```

### Related

- [00064401](#)
- [00064402](#)



## 00065002

### Meaning

An administrator changed an IP reputation setting.

Field name	Description
<b>ID</b>	00065002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:38:03 log_id=00065002 msg_id=000000000171 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed IP Reputation from GUI
(172.20.120.47) "
```

## 00065501

### Meaning

An administrator created an IP reputation exemption.

Field name	Description
<b>ID</b>	00065501
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:38:14 log_id=00065501 msg_id=000000000172 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added IP Reputation Exception 1 from GUI
(172.20.120.47) "
```

### Related

- [00065502](#)
- [00065511](#)

## 00065502

### Meaning

An administrator changed an IP reputation exemption.

Field name	Description
<b>ID</b>	00065502
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=22:51:51 log_id=00065502 msg_id=000000000789 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed IP Reputation Exception 2 from GUI
(192.168.1.28) "
```

### Related

- [00065501](#)
- [00065511](#)

## 00065511

### Meaning

An administrator deleted an IP reputation exemption.

Field name	Description
<b>ID</b>	00065511
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-17 time=22:51:54 log_id=00065511 msg_id=000000000790 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted IP Reputation Exception 2 from GUI
(192.168.1.28) "
```

### Related

- [00065501](#)
- [00065502](#)

## 00068001

### Meaning

An administrator created a combination access control and rate limit rule ("custom rule").

Field name	Description
<b>ID</b>	00068001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-21 time=18:19:40 log_id=00068001 msg_id=000000047914 device_
id=FV400C3M12000060 vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add
status=success msg="User admin added custom-rule Custom_rule_for_PNG_server1 from GUI
(172.22.6.231) "
```

### Related

- [00068002](#)
- [00068011](#)

## 00068002

### Meaning

An administrator changed a combination access control and rate limit rule ("custom rule").

Field name	Description
<b>ID</b>	00068002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-11 time=09:21:30 log_id=00068002 msg_id=000000000441 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed custom-rule combo-IP-rate1 from GUI
(172.20.120.47) "
```

### Related

- [00068002](#)
- [00068011](#)

## 00068011

### Meaning

An administrator deleted a combination access control and rate limit rule ("custom rule").

Field name	Description
<b>ID</b>	00068011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-11 time=09:21:40 log_id=00068011 msg_id=000000000442 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted custom-rule combo-IP-ratel from GUI
(172.20.120.47) "
```

### Related

- [00068001](#)
- [00068002](#)

## 00068301

### Meaning

An administrator created a combination access control and rate limit policy ("custom policy").

Field name	Description
<b>ID</b>	00068301
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-21 time=18:25:26 log_id=00068301 msg_id=000000047918 device_
id=FV400C3M12000060 vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add
status=success msg="User admin added custom-policy Custom_Policy_For_PNG from GUI
(172.22.6.231) "
```

### Related

- [00068302](#)
- [00068311](#)



## 00068302

### Meaning

An administrator changed a combination access control and rate limit policy ("custom policy").

Field name	Description
<b>ID</b>	00068302
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:53:29 log_id=00068302 msg_id=000000000230 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed custom-policy combo-access-
controls1 from GUI(172.20.120.47) "
```

### Related

- [00068301](#)
- [00068311](#)

## 00068311

### Meaning

An administrator deleted a combination access control and rate limit policy ("custom policy").

Field name	Description
<b>ID</b>	00068311
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:53:39 log_id=00068311 msg_id=000000000231 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted custom-policy combo-access-controls1
from GUI(172.20.120.47) "
```

### Related

- [00068301](#)
- [00068302](#)

## 00068401

### Meaning

An administrator has added an padding oracle rule.

Field name	Description
<b>ID</b>	00068401
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=18:19:31 log_id=00068401 msg_id=000000820334 device_
id=FVVM020000018475 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added waf-padding-oracle padding_001 from
GUI (172.22.6.230) "
```

### Related

- [00068402](#)
- [00068411](#)

## 00068402

### Meaning

An administrator edited an padding oracle rule.

Field name	Description
<b>ID</b>	00068402
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=18:24:59 log_id=00068402 msg_id=000000820335 device_
id=FVVM020000018475 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed waf-padding-oracle padding_001 from
GUI (172.22.6.230) "
```

### Related

- [00068401](#)
- [00068411](#)

## 00068411

### Meaning

An administrator deleted an padding oracle rule.

Field name	Description
<b>ID</b>	00068411
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=18:26:05 log_id=00068411 msg_id=000000820336 device_
id=FVVM020000018475 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi"
type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted waf-padding-oracle padding_001 from
GUI (172.22.6.230) "
```

### Related

- [00068401](#)
- [00068402](#)

## 00068701

### Meaning

An administrator added a web cache policy exception.

Field name	Description
<b>ID</b>	00068701
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:44:43 log_id=00068701 msg_id=000000179517 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=add status=success msg="User admin added web-cache-
exception ddd from GUI(172.22.6.66) "
```

### Related

- [00068711](#)
- [00068801](#)
- [00068802](#)
- [00068811](#)

## 00068711

### Meaning

An administrator deleted a web cache policy exception.

Field name	Description
<b>ID</b>	00068711
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-11 time=02:00:30 log_id=00068711 msg_id=000003041973 device_
id=FV400C3M14000006 vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del
status=success msg="User admin deleted web-cache-exception ddd from GUI (172.22.14.6) "
```

### Related

- [00068701](#)
- [00068801](#)
- [00068802](#)
- [00068811](#)

## 00068801

### Meaning

An administrator added a web cache policy.

Field name	Description
<b>ID</b>	00068801
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:41:57 log_id=00068801 msg_id=000000179514 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=add status=success msg="User admin added web-cache-
policy FWB_web_cache from GUI(172.22.6.66) "
```

### Related

- [00068802](#)
- [00068811](#)
- [00068701](#)
- [00068711](#)



## 00068802

### Meaning

An administrator changed a web cache policy.

Field name	Description
<b>ID</b>	00068802
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:43:10 log_id=00068802 msg_id=000000179515 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=edit status=success msg="User admin changed web-
cache-policy FWB_web_cache from GUI(172.22.6.66)"
```

### Related

- [00068801](#)
- [00068811](#)
- [00068701](#)
- [00068711](#)

## 00068811

### Meaning

An administrator deleted a web cache policy.

Field name	Description
<b>ID</b>	00068811
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=16:43:41 log_id=00068811 msg_id=000000179516 device_
id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_
policy="" user=admin ui=GUI action=del status=success msg="User admin deleted web-
cache-policy FWB_web_cache from GUI(172.22.6.66)"
```

### Related

- [00068801](#)
- [00068802](#)
- [00068701](#)
- [00068711](#)

## 00090001

### Meaning

An administrator created a vulnerability scan schedule.

Field name	Description
<b>ID</b>	00090001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:24:24 log_id=00090001 msg_id=000000000140 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added wvs schedule vuln-scan-schedule1 from
GUI(172.20.120.47) "
```

### Related

- [00090002](#)
- [00090011](#)

## 00090002

### Meaning

An administrator changed a vulnerability scan schedule.

Field name	Description
<b>ID</b>	00090002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:24:34 log_id=00090002 msg_id=000000000141 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed wvs schedule vuln-scan-schedule1
from GUI(172.20.120.47) "
```

### Related

- [00090001](#)
- [00090011](#)

## 00090011

### Meaning

An administrator deleted a vulnerability scan schedule.

Field name	Description
<b>ID</b>	00090011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:24:44 log_id=00090011 msg_id=000000000142 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted wvs schedule vuln-scan-schedule1
from GUI(172.20.120.47) "
```

### Related

- [00090001](#)
- [00090002](#)

## 00090101

### Meaning

An administrator created a vulnerability scan profile.

Field name	Description
<b>ID</b>	00090101
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:38:53 log_id=00090101 msg_id=000000734654 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added wvs profile ddddd from GUI(172.22.6.237) "
```

### Related

- [00090102](#)
- [00090111](#)

## 00090102

### Meaning

An administrator changed a vulnerability scan profile.

Field name	Description
<b>ID</b>	00090102
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:29:10 log_id=00090102 msg_id=000000000144 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed wvs profile vuln-scan-profile1 from
GUI(172.20.120.47) "
```

### Related

- [00090101](#)
- [00090111](#)

## 00090111

### Meaning

An administrator deleted a vulnerability scan profile.

Field name	Description
<b>ID</b>	00090111
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-04-10 time=17:42:52 log_id=00090111 msg_id=000000734655 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted wvs profile dddd from GUI(172.22.6.237) "
```

### Related

- [00090101](#)
- [00090102](#)



## 00091101

### Meaning

An administrator created a vulnerability scan policy.

Field name	Description
<b>ID</b>	00091101
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:29:40 log_id=00091101 msg_id=000000000144 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added wvs policy vulnscan1 from GUI
(172.20.120.47) "
```

### Related

- [00091102](#)
- [00091111](#)

## 00091102

### Meaning

An administrator changed a vulnerability scan policy.

Field name	Description
<b>ID</b>	00091102
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:29:50 log_id=00091102 msg_id=000000000145 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed wvs policy vulnscan1 from GUI
(172.20.120.47) "
```

### Related

- [00091101](#)
- [00091111](#)

## 00091111

### Meaning

An administrator deleted a vulnerability scan policy.

Field name	Description
<b>ID</b>	00091111
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:29:59 log_id=00091111 msg_id=000000000146 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted wvs policy vulnscan1 from GUI
(172.20.120.47) "
```

### Related

- [00091101](#)
- [00091102](#)

## 00093001

### Meaning

An administrator created an anti-defacement monitor.

Field name	Description
<b>ID</b>	00093001
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:17:38 log_id=00093001 msg_id=000000000114 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=add status=success msg="User admin added website 1 from GUI(172.20.120.47) "
```

### Related

- [00093002](#)
- [00093011](#)

## 00093002

### Meaning

An administrator changed an anti-defacement monitor.

Field name	Description
<b>ID</b>	00093002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:17:46 log_id=00093002 msg_id=000000000115 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=edit status=success msg="User admin changed website 1 from GUI(172.20.120.47) "
```

### Related

- [00093001](#)
- [00093011](#)

## 00093011

### Meaning

An administrator deleted an anti-defacement monitor.

Field name	Description
<b>ID</b>	00093011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2013-10-08 time=10:17:56 log_id=00093011 msg_id=000000000116 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI
action=del status=success msg="User admin deleted website 1 from GUI(172.20.120.47) "
```

### Related

- [00093001](#)
- [00093002](#)

## 00093501

### Meaning

An administrator created an anti-defacement file filter.

Field name	Description
<b>ID</b>	00093501
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-03 time=11:54:59 log_id=00093501 msg_id=000000003151 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add
status=success msg="User admin added file-filter video_content from GUI (172.20.120.61)
"
```

### Related

- [00093502](#)
- [00093511](#)

## 00093502

### Meaning

An administrator edited an anti-defacement file filter.

Field name	Description
<b>ID</b>	00093502
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-10 time=17:06:02 log_id=00093502 msg_id=000085523288 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-filter video_files from GUI (172.22.14.6) "
```

### Related

- [00093501](#)
- [00093511](#)



## 00093511

### Meaning

An administrator deleted an anti-defacement file filter.

Field name	Description
<b>ID</b>	00093511
(log_id)	See <a href="#">Log ID numbers on page 15</a> .

### Examples

```
date=2014-09-03 time=12:15:06 log_id=00093511 msg_id=000000003152 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=event
subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del
status=success msg="User admin deleted file-filter video_content from GUI
(172.20.120.61) "
```

### Related

- [00093501](#)
- [00093502](#)

## 10000009

### Meaning

An administrator powered on the FortiWeb appliance.

Field name	Description
<b>ID</b>	10000009
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	system
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>Level</b>	information
(pri)	See <a href="#">Priority level on page 16</a> .
<b>Action</b>	start
(action)	

### Examples

```
date=2013-10-08 time=01:33:34 log_id=10000009 msg_id=0000000000007 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada )" type=event
subtype="system)" pri=information trigger_policy="" user=system ui=sys action=start
status=success msg="FortiWeb started"
```

### Related

- [Reboot, shut down, & boot up messages](#)
- [10000010](#)
- [10000011](#)

## 10000010

### Meaning

A FortiWeb administrator rebooted the operating system of the appliance.

If the administrator did this through the web UI, the log message includes the administrator's comment, if he or she provided one.

Field name	Description
<b>ID</b> (log_id)	10000010 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	critical See <a href="#">Priority level on page 16</a> .
<b>Action</b> (action)	reboot
<b>User Interface</b> (ui)	{GUI   none   telnet   ssh   console} Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Message</b> (msg)	User <administrator_name> changed interface <interface_name> from {GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

### Examples

```
date=2013-10-08 time=09:48:54 log_id=10000010 msg_id=0000000000070 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=reboot status=success msg="User admin rebooted the device from GUI (172.20.120.47).This is my comment."
```

**Related**

- [Reboot, shut down, & boot up messages](#)
- [10000009](#)
- [10000011](#)

## 10000011

### Meaning

An administrator halted the operating system of the FortiWeb appliance in preparation to power off the hardware.

Field name	Description
<b>ID</b>	10000011
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	system
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>Level</b>	notification
(pri)	See <a href="#">Priority level on page 16</a> .
<b>Action</b>	shutdown
(action)	

### Examples

```
date=2014-06-16 time=02:41:42 log_id=10000011 msg_id=000000022971 device_
id=FVVM020000018466 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" type=event
subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=shutdown
status=success msg="User admin shut down the device from GUI(172.22.6.241)."
```

### Related

- [Reboot, shut down, & boot up messages](#)
- [10000009](#)
- [10000010](#)

## 10000012

### Meaning

An administrator's inactive session timed out.

Field name	Description
<b>ID</b> (log_id)	10000012 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	notification See <a href="#">Priority level on page 16</a> .
<b>Action</b> (action)	shutdown

### Examples

```
date=2013-10-09 time=20:37:24 log_id=10000012 msg_id=000000000340 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="system)" pri=notification trigger_policy="" user=admin ui=console
action=logout status=success msg="User admin time out on console"
```

### Related

- [10000016](#)

## 10000013

### Meaning

An administrator uploaded a data analytics definition file.

Field name	Description
<b>ID</b> (log_id)	10000013 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information See <a href="#">Priority level on page 16</a> .
<b>Action</b> (action)	update

### Examples

```
date=2014-04-10 time=13:01:33 log_id=10000013 msg_id=000044293782 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin success loaded data analytics file from GUI(10.200.10.80)."
```

## 10000014

### Meaning

An administrator deleted a locally-stored attack log, event log, or traffic log file.

Field name	Description
<b>ID</b> (log_id)	10000014  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	notice  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b> (action)	del
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <administrator_name> has deleted disk log <file_str> from {GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}



### Examples

```
date=2014-04-10 time=18:09:47 log_id=10000014 msg_id=000000195890 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin has deleted disk log elog(2014-04-09-23:34:02).log from GUI(172.22.6.240) "
```

### Related

- [00032006](#)

## 10000015

### Meaning

A FortiWeb administrator downloaded a log file.

Field name	Description
<b>ID</b> (log_id)	10000015  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>User Interface</b> (ui)	GUI
<b>Action</b> (action)	backup
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <administrator_name> download {Attack   Event   Traffic } from GUI (<mgmt_ip>)

### Examples

```
date=2013-10-07 time=16:13:10 log_id=10000015 msg_id=000000001218 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI
action=backup status=success msg="Successfully. User admin download Event LOG from GUI
(172.20.120.47)."
```

## 10000016

**Meaning**

Either a FortiWeb administrator logged in successfully, or attempted to log in but failed.

Field name	Description
<b>ID</b> (log_id)	10000016  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	notification  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from jsconsole indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b> (action)	login
<b>Status</b> (status)	success  failed
<b>Message</b> (msg)	User <administrator_name> logged in successfully from {(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)}  User <administrator_name> login failed from {(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)}

### Examples

```
date=2014-04-10 time=13:31:37 log_id=10000016 msg_id=000044294845 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=admin ui=telnet action=login status=success msg="User admin logged in successfully from telnet (10.200.0.1) "
```

### Related

- [10000012](#)

## 10000017

**Meaning**

Someone attempted to log in to a FortiWeb administrator account, but failed.

**Solution**

If you suspect that an unauthorized person is attempting to log in to your FortiWeb, there are some preventative measures that you can take.

1. Restrict physical access to the FortiWeb to ensure that only authorized persons can attach a console or computer to the appliance's local console port.
2. Configure all administrator accounts with trusted IPs that restrict login attempts to ones that originate **only** from your trusted, physically secured, private administrative network. Do not allow login attempts from hostile or untrusted IP addresses. If **any** administrator account uses a broad trusted IP definition such as 0.0.0.0/0.0.0.0, then due to that account, FortiWeb must allow login attempts from all IP addresses, including the Internet. Brute force login attempts are then a significant risk.
3. Enable strong password enforcement. Passwords must be significantly complex in length and character types in order to make brute force login attempts impractically slow.
4. Require regular password changes.
5. Enable only secure administrative protocols (SSH and HTTPS) on network interfaces. Insecure protocols such as HTTP and Telnet are easily susceptible to eavesdropping, man-in-the-middle, and other attacks that could compromise your connection, your password, or both.

Field name	Description
<b>ID</b>	10000017
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	admin
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>Level</b>	alert
(pri)	See <a href="#">Priority level on page 16</a> .

Field name	Description
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}
<b>Action</b> (action)	login
<b>Status</b> (status)	failure
<b>Message</b> (msg)	User <administrator_name> login failed from {GUI(<mgmt_ip>)   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

### Examples

```
date=2014-04-10 time=18:11:53 log_id=10000017 msg_id=000000195892 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=a ui=GUI action=login status=failed msg="User a login failed from GUI(172.22.6.240)"
```

## 10000018

**Meaning**

A FortiWeb administrator logged out.

Field name	Description
<b>ID</b> (log_id)	10000018  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	notification  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b> (action)	logout
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <administrator_name> logout from {GUI(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

### Examples

```
date=2013-10-08 time=11:25:37 log_id=10000018 msg_id=000000000272 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="system)" pri=information trigger_policy="" user=admin ui=GUI
action=logout status=success msg="User admin logs out from GUI(172.20.120.47)"
```

### Related

- [10000012](#)



## 10000019

### Meaning

A FortiWeb administrator upgraded the firmware image.

Field name	Description
<b>ID</b> (log_id)	10000019  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	critical  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b> (action)	upgrade
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <administrator_name> upgrade the image from {GUI (<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

### Examples

```
date=2014-04-10 time=15:26:51 log_id=10000019 msg_id=000000550016 device_
id=FVVM040000018474 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI
action=upgrade status=success msg="User admin upgrade the image from GUI(10.200.0.1)"
```

### Related

- [10000020](#)

## 10000020

### Meaning

A FortiWeb administrator downgraded the firmware image.

Field name	Description
<b>ID</b> (log_id)	10000020  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	critical  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b> (action)	downgrade
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <administrator_name> downgraded the image from {GUI(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

### Examples

```
date=2014-04-10 time=15:22:38 log_id=10000020 msg_id=000000548987 device_
id=FVVM040000018474 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI
action=downgrade status=success msg="User admin downgraded the image from GUI
(10.200.0.1) "
```

### Related

- [10000019](#)

## 10000021

### Meaning

A FortiWeb administrator restored the system configuration.

Field name	Description
<b>ID</b> (log_id)	10000021  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	critical  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b> (action)	restore
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <administrator_name> downgraded the image from {GUI(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}

**Examples**

```
date=2014-08-06 time=18:37:45 log_id=10000021 msg_id=000016328576 device_id=FV-4KD3R13800048 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=restore status=success msg="User admin restored the configuration from GUI(172.22.6.149)"
```

## 10000022

**Meaning**

A FortiWeb administrator manually requested an update to either the FortiWeb regular virus database, the FortiWeb extended virus database, or the virus engine.

Field name	Description
<b>ID</b> (log_id)	10000022  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	critical  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b> (action)	update
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <administrator_name> manually update {virus signature   virus extend signature   virus engine} from {GUI(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console} success

## Examples

```
date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292728 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin manually update virus signature from GUI (10.200.10.80) success"
```

```
date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292727 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin update virus extend signature from GUI (10.200.10.80) success"
```

```
date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292726 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin update virus engine from GUI (10.200.10.80) success"
```



## 10000023

### Meaning

One of the following events:

- A FortiWeb configuration backup to an FTP/SFTP server either succeeded or failed.
- The scheduled configuration backup daemon started. Normally, this occurs at boot time.
- An administrator downloaded a log file.
- An administrator downloaded a backup of the system configuration file, `fweb_system.conf`.
- An administrator downloaded an X.509 CSR.

### Solution

There could be several reasons why the backup failed.

1. Check the IP address and login credentials that you have defined for FortiWeb's FTP/SFTP connection.
2. Verify that the directory you specified to receive backups exists, and has write permissions for that user name.
3. Make sure that the FTP/SFTP server's disk is not full, that it has enough disk space to receive the backup, and that that user name has not consumed its disk space quota, if any.
4. Verify that FortiWeb's system time is accurate.
5. Make sure that the backup is not scheduled during a network or server maintenance window, when the server or daemon are down.
6. Test that a **reliable** route exists between FortiWeb and the FTP/SFTP server by using `execute ping` and `execute traceroute` commands in the CLI.

Keep in mind that if the network or the server was down for maintenance at the time of the backup attempt, the backup would have failed during that time, even if connectivity works for you now.

7. If you have firewalls or routers performing NAT between FortiWeb and the server, verify that FTP connections are allowed between them. Firewalls include host-based ones that may be on the server itself, such as Windows Firewall or `ipfw`.

Keep in mind that the FTP protocol typically requires port 21, but that its mechanism style could be active or passive FTP, and that the protocol has both a command channel and a data transfer channel. If either of these channels fail, the backup will fail. SFTP typically requires port 22.

Field name	Description
<b>ID</b> (log_id)	10000023 <a href="#">See Log ID numbers on page 15.</a>
<b>Sub Type</b> (subtype)	system <a href="#">See Subtypes on page 16.</a>
<b>User</b> (user)	system
<b>User Interface</b> (ui)	sys
<b>Action</b> (action)	backup start
<b>Message</b> (msg)	backup backup_<FTP-backup_name>_<timestamp_str> to <server_ipv4> <folder_str> {FAIL   OK}

## Examples

```
date=2013-10-08 time=09:42:19 log_id=10000023 msg_id=0000000000038 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )" type=event subtype="system" pri=notification trigger_policy="" user=system ui=sys action=backup status=failed msg="ftp backup backup_scheduled_backup_20131008094215 to ftp.example.com / FAILED"
```

```
date=2013-10-08 time=10:59:14 log_id=10000023 msg_id=000000146032 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=system action=backup msg="backup backup_backup-to-ftp-server_20121113105913 to 172.20.120.225 Downloads/fortiweb/backups/ OK"
```

```
date=2013-10-05 time=19:26:12 log_id=10000023 msg_id=000000001038 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=system ui=sys action=start status=success msg="Backup daemon started"
```

```
date=2014-04-10 time=18:14:52 log_id=10000023 msg_id=000000195894 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the Logging file from GUI (172.22.6.240) "
```

```
date=2014-04-10 time=18:17:06 log_id=10000023 msg_id=000000195895 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the System config file from GUI (172.22.6.240) "
```

```
date=2014-04-10 time=18:18:05 log_id=10000023 msg_id=000000195897 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the Local Cert(CSR) file from GUI (172.22.6.240) "
```

## Related

- [11001008](#)

## 10000027

### Meaning

A FortiWeb administrator changed the system time.

Field name	Description
<b>ID</b> (log_id)	10000027  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	critical  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b> (action)	change-time
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <administrator_name> changed time from <date & time> to <date & time>.

### Examples

```
date=2014-04-10 time=15:13:20 log_id=10000027 msg_id=000044298000 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=console action=change-time status=failed msg="User admin changed time from Thu Apr 10 15:13:06 2014 to Thu Apr 10 15:13:20 2014 ."
```

## 10000028

**Meaning**

A FortiWeb administrator manually updated the IP reputation signature file.

Field name	Description
<b>ID</b>	10000028
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	system
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>Level</b>	critical
(pri)	See <a href="#">Priority level on page 16</a> .
<b>User</b>	<administrator_name>
(user)	
<b>User Interface</b>	{GUI(<mgmt_ip>)   none   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console}
(ui)	Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Action</b>	update
(action)	
<b>Status</b>	success
(status)	
<b>Message</b>	User <administrator_name> manually update IP Reputation signature from time from from {GUI(<mgmt_ip>)   jsconsole   telnet(<mgmt_ip>)   ssh(<mgmt_ip>)   console} success.
(msg)	

**Examples**

```
date=2014-04-10 time=12:54:45 log_id=10000028 msg_id=000044293771 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin manually update IP Reputation signature from GUI(10.200.0.1) success"
```

## 11001008

### Meaning

The logging daemon started. Normally, this occurs at boot time.

Field name	Description
<b>ID</b> (log_id)	11001008 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon
<b>Action</b> (action)	start
<b>Status</b> (status)	success
<b>Message</b> (msg)	Log daemon started

### Examples

```
date=2013-10-05 time=19:26:02 log_id=11001008 msg_id=000000001037 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time (US & Canada) "
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon
action=start status=success msg="Log daemon started"
```

### Related

- [10000023](#)



## 11002003

### Meaning

Someone attempted to log in to a web site where you have configured FortiWeb to provide end-user authentication, but failed.

### Solution

If you suspect that an unauthorized person is attempting to log in to your web site, there are some preventative measures that you can take.

1. Require regular password changes.
2. Require strong passwords. Passwords must be significantly complex in length and character types in order to make brute force login attempts impractically slow.
3. Redirect requests for HTTP to a secure (HTTPS) URL. Insecure protocols such as HTTP are easily susceptible to eavesdropping, man-in-the-middle, and other attacks that could compromise your connection, your password, or both.

Field name	Description
<b>ID</b> (log_id)	11002003 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	alert See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon

Field name	Description
<b>Action</b> (action)	login
<b>Status</b> (status)	failed
<b>Message</b> (msg)	User <user_name> <auth-method_str> login failed from <source_ipv4> request_url: <url>

### Examples

```
date=2014-09-10 time=17:43:31 log_id=11002003 msg_id=000000852763 device_id=FV-3KD3R13800027 vd="Adomain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=login status=failed msg="User test1 HTTP BASIC login failed from 10.0.6.25 request_url:fortinet.fortiweb.com/autotest/ldapuser.html"
```

### Related

- [11002004](#)

## 11002004

### Meaning

An end-user successfully logged in to a web site that you have configured FortiWeb to provide with authentication.

Field name	Description
<b>ID</b> (log_id)	11002004 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon
<b>Action</b> (action)	login
<b>Status</b> (status)	success
<b>Message</b> (msg)	User <user_name> <auth-method_str> login successfully from <source_ipv4> request_url: <url>

### Examples

```
date=2014-09-10 time=17:43:39 log_id=11002004 msg_id=000000852769 device_id=FV-3KD3R13800027 vd="Adomain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumqi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=login status=success msg="User test1 HTTP BASIC login successfully from 10.0.6.25 request_url:fortinet.fortiweb.com/autotest/ldapuser.html"
```

### Related

- [11002003](#)

## 11003601

### Meaning

FortiWeb has detected a change to a web site file that could indicate a defacement attack.

Field name	Description
<b>ID</b> (log_id)	11003601  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon
<b>Action</b> (action)	monitor
<b>Status</b> (status)	success
<b>Message</b> (msg)	File <file_name> on site <site_name> has been changed. Please confirm or restore it.

### Examples

```
date=2014-04-10 time=14:43:11 log_id=11003601 msg_id=000044296936 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=monitor status=failed msg="File [/sig-db/signature.db] on site [2] has been changed. Please confirm or restore it."
```

## 11004002

### Meaning

FortiWeb failed to connect to a web site that you have configured to be monitored by the anti-defacement feature. Therefore it could not determine whether or not the web site has been defaced.

### Solution

If anti-defacement could not connect to the web site:

1. Verify the login and IP address that you provided.
2. On the web server, check the file system permissions for the account that FortiWeb is using to connect. (FortiWeb must be able to both read and, if it will be restoring files, write to the folder and files.
3. On Microsoft Windows, you may need to examine your security policy configuration to make sure that the account is authenticating as itself, and is not degrading to the guest account.)
4. Verify that a route exists between the FortiWeb and the web server, and that connectivity is reliable, with no packet loss.
5. Verify that any routers or firewalls between the appliance and the server, including Windows Firewall, are not blocking SSH, FTP, or CIFS connections.
6. Other troubleshooting varies by the protocol that FortiWeb is using to connect, such as checking for a compatible protocol version and cipher suite.

Field name	Description
<b>ID</b>	11004002
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	admin
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>Level</b>	warning
(pri)	See <a href="#">Priority level on page 16</a> .
<b>User Interface</b>	anti-defacement
(ui)	

Field name	Description
<b>Action</b> (action)	monitor
<b>Status</b> (status)	alert
<b>Message</b> (msg)	Fail to connect to website <anti-defacement_name> (host is <server_ipv4>)

### Examples

```
date=2012-02-13 time=18:49:09 log_id=00032901 msg_id=000015400628 type=event
subtype="admin" pri=warning device_id=FV-1KC3R08600008 vd="root" timezone="(GMT+8:00)
Beijing,ChongQing,HongKong,Urumgi" ui=anti-defacement action=monitor status=alert
reason=filechange msg="Fail to connect to website www.example.com (host is 10.0.0.1)"
```

## 11004601

### Meaning

A failover occurred — that is, the secondary (standby) appliance in the FortiWeb high availability (HA) cluster assumed the duties of processing traffic because it detected that the primary (active) appliance had failed.

Field name	Description
<b>ID</b> (log_id)	11004601 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon
<b>Action</b> (action)	HA-Switch
<b>Status</b> (status)	success
<b>Message</b> (msg)	HA switch from standby to main.

### Examples

```
date=2014-04-10 time=14:35:54 log_id=11004601 msg_id=000044296931 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-Switch status=success msg="HA switch from standby to main."
```



**Related**

- [11004602](#)
- [11004603](#)
- [11004605](#)
- [11004606](#)
- [11004608](#)

## 11004602

### Meaning

An administrator has manually synchronized configuration files from the active HA appliance to the standby appliance.

Field name	Description
<b>ID</b> (log_id)	11004602  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>User</b> (user)	admin
<b>User Interface</b> (ui)	console
<b>Action</b> (action)	HA-Synchronize
<b>Status</b> (status)	success
<b>Message</b> (msg)	User admin synchronize the waf configuration to standby device from console.

### Examples

```
date=2014-04-10 time=14:55:59 log_id=11004602 msg_id=000044296940 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=console action=HA-Synchronize status=success msg="User admin synchronize the waf configuration to standby device from console."
```

**Related**

- [11004601](#)
- [11004603](#)
- [11004605](#)
- [11004606](#)
- [11004608](#)

## 11004603

### Meaning

An appliance has been added to or removed from the high availability (HA) cluster.

Field name	Description
<b>ID</b> (log_id)	11004603 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon
<b>Action</b> (action)	HA-member-left
<b>Status</b> (status)	success
<b>Message</b> (msg)	Member <device_id> {left   join to the} HA group.

### Examples

```
date=2014-04-10 time=15:37:31 log_id=11004603 msg_id=000044298015 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-member-left status=success msg="Member (FV-1KD3A13800001) left HA group."
```

```
date=2014-04-10 time=15:38:42 log_id=11004603 msg_id=000044298021 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-member-join status=success msg="Member (FV-1KD3A13800001) join to the HA group."
```

**Related**

- [11004601](#)
- [11004602](#)
- [11004605](#)
- [11004606](#)
- [11004608](#)

## 11004605

### Meaning

In a high availability (HA) cluster, the configuration has been restored from the active (master) to the standby (slave) appliance.

Field name	Description
<b>ID</b> (log_id)	11004605  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon
<b>Action</b> (action)	restore
<b>Status</b> (status)	success
<b>Message</b> (msg)	HA restored the configuration from master : <device_id>

### Examples

```
date=2014-04-10 time=15:56:40 log_id=11004605 msg_id=000000187139 device_id=FV-1KD3A13800001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=restore status=success msg="HA restored the configuration from master : FV-1KD3A13800002"
```

**Related**

- [11004601](#)
- [11004602](#)
- [11004603](#)
- [11004606](#)
- [11004608](#)

## 11004606

### Meaning

In a high availability (HA) cluster, the firmware has been restored from the active (master) to the standby (slave) appliance.

Field name	Description
<b>ID</b> (log_id)	11004606 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon
<b>Action</b> (action)	restore
<b>Status</b> (status)	success
<b>Message</b> (msg)	HA restored the image from master : <device_id>

### Examples

```
date=2014-04-10 time=16:49:38 log_id=11004606 msg_id=000000188232 device_id=FV-1KD3A13800001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=restore status=success msg="HA restored the image from master : FV-1KD3A13800002"
```



**Related**

- [11004601](#)
- [11004602](#)
- [11004603](#)
- [11004605](#)
- [11004608](#)

## 11004608

### Meaning

In a high availability (HA) cluster, the up/down status of the port that is monitored for link failure has changed..

Field name	Description
<b>ID</b> (log_id)	11004608 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	daemon
<b>Action</b> (action)	HA-monitor-port
<b>Status</b> (status)	success
<b>Message</b> (msg)	HA monitor port <port_name> status changed from down to up.

### Examples

```
date=2014-09-11 time=18:30:41 log_id=11004608 msg_id=000085524326 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-monitor-port status=success msg="HA monitor port (port4) status changed from up to down."
```

```
date=2014-09-11 time=18:30:35 log_id=11004608 msg_id=000085524325 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-monitor-port status=success msg="HA monitor port (port4) status changed from down to up."
```

### Related

- [11004601](#)
- [11004602](#)
- [11004603](#)
- [11004605](#)
- [11004606](#)

## 11005901

### Meaning

Either:

- the FortiGuard Antivirus, FortiGuard FortiWeb Security Service, or FortiGuard IP Reputation Intelligence Service (IRIS) license could not be authenticated
- the FortiGuard services were up-to-date as of the time when FortiWeb polled FortiGuard for updates
- FortiWeb could not connect to the FDN update servers, or the connection was interrupted, and therefore could not update its packages for FortiGuard services
- a FortiGuard service update installation failed
- a FortiGuard service update succeeded
- License authentication determined that the FortiWeb-VM license uploaded by an administrator is either valid or invalid.

## Solution

If a FortiGuard license could not be authenticated:

1. Check with the [Fortinet Technical Support web site](#) to make sure that you have purchased a license for this FortiWeb. If you have an HA pair, you should have one license for each appliance in the pair.
2. Verify that the license is not currently expired, or not yet in effect.
3. Verify that FortiWeb can connect to the Internet to validate its license. To do this, it will require a valid route, DNS settings, and possibly also time settings. If connectivity is unreliable, the initial license request may fail. In this case, you can either wait 30 minutes for the appliance to request authorization again, or use the CLI command `execute update-now` to force an immediate license authentication query.

If FortiWeb could not connect to the FDN or package retrieval failed, verify that FortiWeb has reliable Internet connectivity.

If the license is invalid:

1. Check with the [Fortinet Technical Support web site](#) to make sure that you have purchased a license for this FortiWeb. If you have an HA pair, you should have one license for each appliance in the pair. If you are using a trial license, verify that the trial period has not expired.
2. If you are using a purchased license, verify that you have uploaded the license file to FortiWeb-VM.
3. Verify that the license has not been already used by another. (If you upload the license and it is currently associated with a different management IP, the web UI will display an error message: `Duplicate license detected.`)
4. Verify that the number of allocated vCPUs does not exceed the limit of the license.

Verify that FortiWeb can connect to the Internet to validate its license. To do this, it will require a valid route, DNS settings, and possibly also time settings. If connectivity is unreliable, the initial license request may fail. In this case, you can either wait 30 minutes for the appliance to request authorization again, or use the CLI command `execute update-now` to force an immediate license authentication query.

Field name	Description
<b>ID</b>	11005901
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	system
(subtype)	See <a href="#">Subtypes on page 16</a> .

Field name	Description
<b>Level</b> (pri)	<p>error (for unauthorized licenses, update failures, or connectivity errors)</p> <p>information (for up-to-date results from the FortiGuard poll)</p> <p>critical (for invalid license)</p> <p>See <a href="#">Priority level on page 16</a>.</p>
<b>Message</b> (msg)	<p>Fortiweb {ip intelligence signature   virus engine   virus extend signature   virus signature   waf signature} is unauthorized</p> <p>Fortiweb {ip intelligence signature   virus engine   virus extend signature   virus signature   waf signature} is already up-to-date</p> <p>update failed, failed to connect to fds server!</p> <p>update failed, couldn't receive a update package!</p> <p>Fortiweb {ip intelligence signature   virus engine   virus extend signature   virus signature   waf signature} update failed</p> <p>Fortiweb {ip intelligence signature   virus engine   virus extend signature   virus signature   waf signature} update succeeded</p> <p>License status changed to {VALID   INVALID}</p>

## Examples

```
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000195866 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus engine is unauthorized"
```

```
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000123728 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus extend signature is unauthorized"
```

```
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000123727 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus signature is unauthorized"
```

```
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000146653 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb waf signature is already up-to-date"
```

## Examples

```
Fortiweb waf signature is unauthorized
date=2014-04-10 time=16:00:02 log_id=11005901 msg_id=000000734617 device_id=FV-
1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event
subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update
status=failed msg="Fortiweb waf signature is unauthorized"
```

```
date=2014-04-10 time=16:00:02 log_id=11005901 msg_id=000000734621 device_id=FV-
1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event
subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update
status=failed msg="Fortiweb ip intelligence signature is unauthorized"
```

```
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000189416 device_id=FV-
1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon
action=update status=failed msg="Fortiweb ip reputation signature is already up-to-
date"
```

```
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000158889 device_id=FV-
1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon
action=update status=failed msg="update failed failed to connect fds server!"
```

```
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000070564 device_id=FV-
1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon
action=update status=failed msg="Fortiweb virus extend signature update failed"
```

```
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000068286 device_id=FV-
1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon
action=update status=failed msg="Fortiweb virus engine update succeeded"
```

```
date=2014-04-10 time=09:36:15 log_id=11005901 msg_id=000000022248 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event
subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update
status=failed msg="License status changed to VALID"
```

```
date=2014-04-10 time=09:36:15 log_id=11005901 msg_id=000000104120 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event
subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update
status=failed msg="License status changed to INVALID"
```

## 11006004

### Meaning

A FortiWeb administrator brought up or brought down a network interface,

Field name	Description
<b>ID</b> (log_id)	11006004 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	information See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	daemon
<b>User Interface</b> (ui)	none
<b>Action</b> (action)	check-resource
<b>Status</b> (status)	failed
<b>Message</b> (msg)	interface <interface_name> link {up   down}



### Examples

```
date=2013-10-08 time=09:48:12 log_id=11006004 msg_id=0000000000068 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none
action=check-resource status=failed msg="interface port2 link up"
```

```
date=2013-10-08 time=14:09:10 log_id=11006004 msg_id=0000000000286 device_
id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada )"
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none
action=check-resource status=failed msg="interface vlan3 link down"
```

### Related

- [00004401](#)
- [00004402](#)
- [00004411](#)

## 11006005

### Meaning

Either the CPU usage:

- became too high and exceeded the alert threshold, or
- lowered until it did not exceed the alert threshold anymore

Field name	Description
<b>ID</b>	11006005
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	system
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>User</b>	daemon
(user)	
<b>User Interface</b>	none
(ui)	
<b>Action</b>	check-resource
(action)	
<b>Status</b>	failed
(status)	
<b>Message</b>	CPU usage raise too high,CPU(<percentage_int>)
(msg)	CPU usage reduced,CPU(<percentage_int>)

### Examples

```
date=2013-10-05 time=20:26:59 log_id=11006005 msg_id=000000001043 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none
action=check-resource status=failed msg="CPU usage raise too high,CPU(96)"
```

```
date=2013-10-07 time=15:29:35 log_id=11006005 msg_id=000000001207 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none
action=check-resource status=failed msg="CPU usage reduced, CPU usage is 53"
```

### Related

- [00032006](#)
- [11006006](#)

## 11006006

### Meaning

Either the RAM usage:

- became too high and exceeded the alert threshold, or
- lowered until it did not exceed the alert threshold anymore

Field name	Description
<b>ID</b>	11006006
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	system
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>User</b>	daemon
(user)	
<b>User Interface</b>	none
(ui)	
<b>Action</b>	check-resource
(action)	
<b>Status</b>	failed
(status)	
<b>Message</b>	mem usage raise too high,mem(<usage_int>)
(msg)	mem usage reduced,mem(<usage_int>)

### Examples

```
date=2013-10-05 time=20:26:59 log_id=11006006 msg_id=000000001042 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none
action=check-resource status=failed msg="mem usage raise too high,mem(96)"
```

```
date=2013-10-05 time=20:29:06 log_id=11006006 msg_id=000000001048 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none
action=check-resource status=failed msg="mem usage reduced,mem(52)"
```

### Related

- [00032006](#)
- [11006005](#)

## 11006701

### Meaning

A certificate revocation list (CRL) has been updated using a query to a server.

Field name	Description
<b>ID</b> (log_id)	11006701 See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	notice See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	system
<b>User Interface</b> (ui)	none
<b>Action</b> (action)	edit
<b>Status</b> (status)	success
<b>Message</b> (msg)	A CRL is updated crl=<crl_name> method=HTTP

### Examples

```
date=2014-04-10 time=17:14:18 log_id=11006701 msg_id=000000179557 device_
id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
type=event subtype="system" pri=notice trigger_policy="" user=system ui=none
action=edit status=success msg=" A CRL is updated crl=CRL_4 method=HTTP"
```

**Related**

- [00008801](#)
- [00008811](#)
- [00009301](#)
- [00009311](#)

## 19999496

### Meaning

A web server that belongs to a server pool definition became available (up) or unavailable (down) according to the configured server health check, if any.

### Solution

If a web server is being detected as unavailable, but it is actually up:

Verify that you have selected a server health check in the server pool definition.

Verify that the server health check is using a method to contact the server that the server can respond to. If you are using **Ping**, for example, the server must be responsive to ICMP `ECHO_REQUEST` signals.

Field name	Description
<b>ID</b> (log_id)	19999496  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	alert  See <a href="#">Priority level on page 16</a> .
<b>User</b> (user)	<administrator_name>
<b>User Interface</b> (ui)	{GUI   none   telnet   ssh   console}  Logins from <code>jsconsole</code> indicate use of the <b>CLI Console</b> widget on <b>System &gt; Status &gt; Status</b> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
<b>Message</b> (msg)	policy <policy_name> Physical Server[<pserver_name>:<pserver-port_int>] is {down   up}



## Examples

```
date=2013-10-07 time=12:27:45 log_id=19999496 msg_id=000000001136 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon
action=check-resource status=failed msg="policy policy1 Physical Server[apache1:80] is
up"
```

```
date=2013-10-05 time=19:26:44 log_id=19999496 msg_id=000000001039 device_
id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"
type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon
action=check-resource status=failed msg="policy policy1 Physical Server[apache1:80] is
down"
```

## Related

- [00040001](#)
- [00040002](#)
- [00040011](#)

## 19999497

### Meaning

The number of concurrent sessions has been reduced. For more information on model- or configuration-dependent limits, see the [FortiWeb Administration Guide](#).

Field name	Description
<b>ID</b>	19999497
(log_id)	See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b>	system
(subtype)	See <a href="#">Subtypes on page 16</a> .
<b>Level</b>	alert
(pri)	See <a href="#">Priority level on page 16</a> .
<b>Message</b>	
(msg)	policy <policy_name> concurrent session reduced

### Examples

```
date=2014-04-10 time=18:04:19 log_id=19999497 msg_id=000044306075 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri>alert trigger_policy="" user=daemon ui=daemon action=none status=failed msg="policy test concurrent session reduced"
```

### Related

- [19999498](#)

## 19999498

### Meaning

The maximum number of concurrent sessions has been reached. For more information on model- or configuration-dependent limits, see the [FortiWeb Administration Guide](#).

Field name	Description
<b>ID</b> (log_id)	19999498  See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	system  See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	alert  See <a href="#">Priority level on page 16</a> .
<b>Message</b> (msg)	policy <policy_name> concurrent session exceed threshold

### Examples

```
date=2014-04-10 time=18:03:39 log_id=19999498 msg_id=000044305882 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=check-resource status=failed msg="policy test concurrent session exceed threshold"
```

### Related

- [19999497](#)

# Attack

Attack log messages record traffic that violated its matching policy. Log ID numbers of this type are listed in the table [Attack logs by subtype & ID](#).

The operating mode, network topology, and the rule's configured **Action** can all affect how a policy responds to an attack, data leak, or server information disclosure. Depending on your configuration, violating traffic is either:

- blocked
- sanitized, then passed through
- allowed to continue unmodified (that is, logged only)

FortiWeb does not record the following types of attack logs individually. Instead, it records them periodically while the attack is ongoing, even if the attack has multiple sources:

- DoS attacks
- Padding oracle attacks
- HTTP/HTTPS protocol constraints

This aggregation prevents FortiWeb from flooding attack logs with identical or very similar messages. To differentiate logs caused by individual attacks from those caused by multiple attacks in the same category, FortiWeb records whether it generated the attack log message after matching multiple signatures.

In the attack log, the message field of aggregated log messages displays the message `rule_name : Custom Access Violation`.

In aggregated attacks log, the type field displays the message `Multiple Custom access rule Violations`.

To locate a description for an attack log message, match the **ID** (`log_id`) field in the attack log message with that shown in the table [Attack logs by subtype & ID](#). All attack log messages have the same body fields, described in [Attack log fields on page 392](#).

For attack log messages generated by a HTTP protocol constraint, the associated policy name is displayed in the raw view (`[policy_name:<protocol_constraint_name>]`) but not in the formatted view.

## Attack logs by subtype & ID

ID (log_id)	Sub Type (subtype)	Message (msg)
20000001	waf_allow_method	HTTP Method Violation
20000002	allow_host	HTTP Host Violation
20000003	waf_page_rule	Page Access Rule Violation
20000004	waf_start_page	Start Page Violation

ID (log_id)	Sub Type (subtype)	Message (msg)
20000005	waf_cookie_poison	cookie name (<parameter_name>) : Cookie Poisoning [ <original_value> -> <corrupted_value>; Domain: <domain>; Path: <path>
20000006	waf_parameter_rule	Parameter Validation Violation: (<parameter_name>)
20000007	waf_black_ip	Blacklisted IP blocked
20000008	waf_url_access	<rule_name>: URL Access Violation
20000009	waf_custom_signature_match	Custom Signature Detection: <custom_ signature_rule_name>
20000010 waf_signature_detection		Credit Card Detection : Signature ID <b>n</b>
		Cross Site Scripting : Signature ID <b>n</b>
		Cross Site Scripting(Extended) : Sig- nature ID <b>n</b>
		Generic Attacks-<subtype_name> : Sig- nature ID <b>n</b>
		Generic Attacks(Extended)-<subtype_ name> : Signature ID <b>n</b>
		Information Disclosure-<subtype_ name>: Signature ID <b>n</b>
		KnownExploits-<subtype_name>: Sig- nature ID <b>n</b>
		SQL Injection : Signature ID <b>n</b>  where <b>n</b> is the index number of the specific predefined attack or data leak signature
		SQL Injection(Extended) : Signature ID <b>n</b>
		Bad Robot : Signature ID <b>n</b>
		Trojans : Signature ID <b>n</b>

ID (log_id)	Sub Type (subtype)	Message (msg)
20000019	waf_hidden_fields	Hidden Field Manipulation
20000018	waf_brute_login	Brute Force Login Violation
20000030	waf_custom_access	<b>&lt;custom_rule_name&gt;</b> : Custom Access Violation
20000032	waf_header_overflow	[policy_name: <b>&lt;protocol_constraint_name&gt;</b> ] :Header Length Exceeded: (the current header length <b>n</b> exceeded the maximum header length limitation <b>n</b> )
20000033	waf_headline_overflow	[policy_name: <b>&lt;protocol_constraint_name&gt;</b> ] :Header Line Length Exceeded: (the current HTTP header line length <b>n</b> exceeded the maximum length limitation <b>n</b> )
20000034	waf_body_overflow	[policy_name: <b>&lt;protocol_constraint_name&gt;</b> ] :Body Length Exceeded: (the current HTTP body length <b>n</b> exceeded the maximum HTTP body length limitation <b>n</b> )
20000035	waf_content_overflow	[policy_name: <b>&lt;protocol_constraint_name&gt;</b> ] : Content Length Exceeded: (the current content length <b>n</b> exceeded the maximum content length limitation <b>n</b> )
20000036	waf_parameter_overflow	[policy_name: <b>&lt;protocol_constraint_name&gt;</b> ] : Total URL and Body Parameters Length Exceeded: (the current URL and body length <b>n</b> exceeded the maximum length limitation <b>n</b> )
20000037	waf_request_overflow	[policy_name: <b>&lt;protocol_constraint_name&gt;</b> ] : HTTP Request Length Exceeded: (the current request length <b>n</b> exceeded the maximum request length limitation <b>n</b> )

ID (log_id)	Sub Type (subtype)	Message (msg)
20000038	waf_url_parameter_overflow	[policy_name:<protocol_constraint_name>] : Total URL Parameters Length Exceeded: (the current URL parameter length <b>n</b> exceeded the maximum length limitation <b>n</b> )
20000039	waf_illegal_http_version	[policy_name:<protocol_constraint_name>] : Illegal HTTP Version
20000040	waf_cookiecount_overflow	[policy_name: <protocol_constraint_name>] : Too Many Cookies in Request: (cookie number <b>n</b> exceeded the maximum cookie number limitation <b>n</b> )
20000041	waf_req_headline_overflow	[policy_name:<protocol_constraint_name>] : Too Many Headers In Request: (header line number <b>n</b> exceeded the maximum header line number limitation <b>n</b> )
20000042	waf_ip_reputation	IP Reputation Violation: <category_name>
20000043	waf_url_parameter_count_overflow	[policy_name:<protocol_constraint_name>] : Too Many Parameters in Request: (the current parameter number <b>n</b> exceeded the maximum parameter number limitation <b>n</b> )
20000044	waf_illegal_hostname	[policy_name:<protocol_constraint_name>] : Illegal Host Name: (host name <host> is illegal)
20000045	waf_illegal_file_type	filename [<file_str>]: Illegal file size/type
20000046 (when based upon the HTTP session ID)	DDOS based on HTTP session: waf_http_request_overflow	DoS Attack: HTTP Flood Prevention Violation
20000047 (when based upon the source IP)	DDOS based on HTTP session: waf_tcp_connection_overflow	DoS Attack: Malicious IPs Violation

ID (log_id)	Sub Type (subtype)	Message (msg)
20000048	waf_max_num_ranges_in_Range_header	[policy_name:<protocol_constraint_name>] : Too Many Range Headers: (the range header number <b>n</b> exceeded the maximum range header number <b>n</b> )
20000049	http_protocol_error	[policy_name:<protocol_constraint_name>] : Malformed Request - Header Too Large : Malformed Request  or  [policy_name:<protocol_constraint_name>] : Malformed Request - Parameter Too Large : Malformed Request
20000050 (when based upon the HTTP session ID)	DDOS based on source IP: waf_http_request_overflow	DoS Attack: HTTP Access Limit Violation
20000051 (when based upon the source IP)	DDOS based on source IP: waf_tcp_connection_overflow	DoS Attack: TCP Flood Prevention Violation
20000052	https_connection_failed	Varies by the cause of the SSL/TLS error. See <a href="#">SSL/TLS error messages on page 395</a> .
20000053	waf_padding_oracle	Padding Oracle Attack
20000055	fsa_detection	Malicious file detected by FortiSandbox
21000022	waf_dos_prevention_type	DoS Attack: SYN Flood  DoS Attack: SYN Flood Stopped

## Attack log fields

Fields in the body of attack log messages are described below.

For descriptions of header fields that exist in every log message, see [Header & body fields on page 5](#).



### Meaning

Traffic violating a policy was detected by the FortiWeb appliance.

### Solution

If your appliance was:

- operating in reverse proxy or true transparent proxy mode **and**
- configured to **deny** traffic (e.g. the **Action** is **Alert & Deny** in the log message)

the traffic was blocked. **No action is required.** If many attacks come from a client, though, for performance reasons, consider blacklisting its IP address.

Otherwise, if your appliance was:

- operating in offline protection or transparent inspection mode **or**
- configured only to **monitor** traffic (e.g. **Monitor Mode** was enabled or the **Action** is **Alert**, not **Alert & Deny**)

examine the web server to determine whether or not it was affected.

By the nature of log-only actions, detected attack attempts are logged but **not** blocked. You may also want to determine if the attack is from a single source IP address or distributed: blacklisting an offending client may help you to efficiently prevent further attack attempts, improving performance, until you can take further action.

By the nature of the network topology for offline protection mode (which can potentially cause differences in speeds of the separate routing paths), and asynchronous inspection for transparent inspection mode, **blocking cannot be guaranteed.** For details, see the [FortiWeb Administration Guide](#).

**Tip:** If an attack is not being detected as you expect, enable session management, traffic logging, and packet payload retention. You can examine the traffic log's packet payload to determine why it is not matching your profile rules and/or enabled attack signatures. For instructions, see the [FortiWeb Administration Guide](#).

Field name	Description
<b>ID</b> (log_id)	An identifying number. See <a href="#">Log ID numbers on page 15</a> and the column <b>ID</b> on page 388.
<b>Sub Type</b> (subtype)	See <a href="#">Subtypes on page 16</a> and the column <b>Sub Type</b> on page 388.
<b>Level</b> (pri)	alert

Field name	Description
<b>Action</b> (action)	<p>The action that you configured FortiWeb to take in response to the policy violation, such as:</p> <p>Alert</p> <p>or</p> <p>Alert_Deny</p> <p>Action options vary by the nature of the attack. For details on actions, see the <a href="#">FortiWeb Administration Guide</a>.</p>
<b>Service</b> (service)	<p>&lt;service_name&gt;</p>
<b>Policy</b> (policy)	<p>&lt;server-policy_name&gt;</p>
<b>Method</b> (http_method)	<p>Varies by the web application, but is usually GET or POST.</p>
<b>HTTP Host</b> (http_host)	<p>The domain name as it appears in the request from the client. This name can be different from your internal DNS name, if any, for the web server, or, if you are using HTTP Host: rewrites, different from the domain name of the virtual host on the web server. (For example, www.example.co.jp instead of www1.local or the virtual host that serves responses for all DNS names, www.example.com.)</p>
<b>URL</b> (http_url)	<p>The URL as it appears in the request from the client. Can be a rewritten URL. This URL does not include the service or host name (for example, /main/index.html).</p>
<b>User Agent</b> (http_agent)	<p>The HTTP client platform, as it is reported by the client itself. This is often fake in attacks.</p>
<b>HTTP Session ID</b> (http_session_id)	<p>The HTTP session identifier associated with the HTTP request (if any).</p> <p>The ID may be <code>unknown</code> if the Session Management option is not enabled in the governing protection profile.</p>
<b>Message</b> (msg)	<p>See the column <a href="#">Message on page 388</a>.</p>
<b>Signature Subclass</b> (signature_subclass)	<p>The name of the signature subclass.</p> <p>If the current signature has no subclass, the main class is displayed.</p>

Field name	Description
<b>Signature ID</b> (signature_id)	The ID of the specific signature within the subclass that triggered the log message.
<b>Source Country</b> (srccountry)	The country that is the source of the traffic.
<b>HTTP Content Routing</b> (content_switch_name)	The name of the associated HTTP content routing policy.
<b>Server Pool</b> (server_pool_name)	The name of the server pool in the associated server policy.

### Example

```
date=2014-06-22 time=23:52:38 log_id=20000010 msg_id=000000102972 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=attack subtype="waf_signature_detection" pri=alert trigger_policy="" severity_level=Low proto=tcp service=http action=Alert policy="Auto-policy" src=10.0.8.103 src_port=1114 dst=10.20.8.22 dst_port=80 http_method=get http_url="/" http_host="10.0.8.22" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; " http_session_id=none msg="[Signatures name: FWB_server_protection] [main class name: Information Disclosure] [sub class name: HTTP Header Leakage]: 080200004" signature_subclass="HTTP Header Leakage" signature_id="080200004" srccountry="Reserved" content_switch_name="none" server_pool_name="Auto-ServerFarm"
```

## SSL/TLS error messages

If you are configuring HTTPS for the first time, and there are configuration errors still, you might see some SSL or TLS-related error messages. Because they are rare and tend to indicate a potential attack attempt, they are located in the attack logs, except for cipher or key exchange errors, which tend to be traffic flow problems (see [Traffic on page 399](#)).

Although the **ID** (log\_id) is the same for all HTTPS connection errors (**20000052**), the **Message** (msg) field varies by the cause.

**HTTPS attack log messages**

Message (msg)	Cause & description
X509 Error 2 - Unable to get issuer certificate	The CA's certificate does not exist in the store of trusted CAs ( <b>System &gt; Certificates &gt; CA</b> ), nor is it included in a signing chain within the certificate file.
X509 Error 3 - Unable to get certificate CRL	Unable to get certificate CRL. The CRL of a certificate could not be found. Unused.
X509 Error 4 - The certificate signature could not be decrypted.	The certificate's signature value could not be determined, and therefore it could not be decrypted. It does <b>not</b> mean that the signature did not match the expected value.  This applies only to RSA keys.
X509 Error 5 - The CRL signature could not be decrypted	Unable to decrypt CRL's signature the CRL signature could not be decrypted: this means that the actual signature value could not be determined rather than it not matching the expected value. Unused.
X509 Error 6 - Unable to decode issuer public key	The public key in the certificate's CA's <code>Subject Public Key Info:</code> field could not be read.
X509 Error 7 - Certificate signature failure	The certificate's signature is invalid.
X509 Error 8 - CRL signature failure	The signature of the certificate in the CRL is invalid. Unused.
X509 Error 9 - Certificate is not yet valid	The certificate's <code>Not Before:</code> field is after the current time and date.
X509 Error 10 - Certificate has expired	The certificate's <code>Not After:</code> field is after the current time and date.
X509 Error 11 - CRL is not yet valid	CRL is not yet valid the CRL is not yet valid. Unused.
X509 Error 12 - CRL has expired	CRL has expired the CRL has expired. Unused.
X509 Error 13 - Format error. The certificate notBefore field contains an invalid time	The certificate's <code>Not Before:</code> field contains an invalid time.
X509 Error 14 - Format error. The certificate notAfter field contains an invalid time	The certificate's <code>Not After:</code> field contains an invalid time.

Message (msg)	Cause & description
X509 Error 15 - Format error. The CRL <code>lastUpdate</code> field contains an invalid time	Format error in URL's <code>lastUpdate</code> field. The CRL <code>lastUpdate</code> field contains an invalid time. Unused.
X509 Error 16 - Format error. The CRL <code>nextUpdate</code> field contains an invalid time	Format error in CRL's <code>nextUpdate</code> field. The CRL <code>nextUpdate</code> field contains an invalid time. Unused.
X509 Error 17 - An error occurred trying to allocate memory	FortiWeb is out of memory. This should never happen.
X509 Error 18 - Certificate is self signed and the same certificate cannot be found in the list of trusted certificates	The certificate is self-signed meaning that it is acting as its own CA. However, the certificate does not exist in the store of trusted CAs ( <b>System &gt; Certificates &gt; CA</b> ).
X509 Error 19 – Root certificate could not be found locally	The certificate contains a signing chain that is not complete. The certificate's signing chain must terminate with the certificate of a CA that is trusted by FortiWeb ( <b>System &gt; Certificates &gt; CA</b> ).
X509 Error 20 - Issuer certificate could not be found	The certificate indicates an <code>Issuer:</code> field (CA), so it should not be self-signed. However, the certificate's signing chain does not contain that issuing CA's certificate.
X509 Error 21 - No signatures could be verified. Chain contains only one certificate and it is not self signed	The certificate's signing chain contains only one certificate. However, the certificate is not a self-signed certificate.
X509 Error 22 - Certificate chain too long	The certificate chain length is greater than the supplied maximum depth. Unused.
X509 Error 23 - The certificate has been revoked	The certificate has been revoked. Unused.
X509 Error 24 - Invalid CA certificate	Either the CA's certificate is not actually from a CA, or its extensions are not consistent with the supplied purpose.
X509 Error 25 - Path length constraint exceeded	The certificate's <code>Basic Constraints: field's Path Length Constraint=</code> parameter was exceeded.
X509 Error 26 - Unsupported certificate	The certificate's <code>Key Usage: field</code> or <code>Enhanced Key Usage: field</code> does not match FortiWeb's purpose. This could occur if, for example, an email signing certificate were to be accidentally used as a server certificate.

Message (msg)	Cause & description
X509 Error 27 - Certificate not trusted	The root CA's certificate is not marked as trusted for the certificate's purpose ( <code>Certificate Usage: field</code> ).
X509 Error 28 - Certificate rejected.	The root CA's certificate is marked to reject the certificate's purpose ( <code>Certificate Usage: field</code> ).
X509 Error 29 - Subject issuer mismatch	The current candidate issuer certificate was rejected because its <code>Subject: name</code> did not match the <code>Issuer: name</code> of the current certificate. Only displayed when the <code>-issuer_checks</code> option is set.
X509 Error 30 - Authority and subject key identifier mismatch	The current candidate issuer certificate was rejected because its <code>Subject Key Identifier: was present</code> and did not match the <code>Authority Key Identifier: current certificate</code> . Only displayed when the <code>-issuer_checks</code> option is set.
X509 Error 31 - Authority and issuer serial number mismatch	The current candidate issuer certificate was rejected because its <code>Issuer: name</code> and <code>Serial Number: field</code> was present and did not match the <code>Authority Key Identifier: of the current certificate</code> . Only displayed when the <code>-issuer_checks</code> option is set.
X509 Error 32 - Key usage does not include certificate signing	The certificate of the CA currently being examined in the signing chain was rejected because its <code>Key Usage: extension</code> does not permit certificate signing.
X509 Error 50 - Application verification failure	Application verification failure an application specific error. Unused.
X509 Error 52 - Get client certificate failed	FortiWeb does not have the certificate of the CA that signed the personal certificate in its store of trusted CAs ( <b>System &gt; Certificates &gt; CA</b> ), and therefore cannot verify the personal certificate.
X509 Error 53 - Protocol error	The client did not present its personal certificate to FortiWeb. This could be caused by the client not having its personal certificate properly installed.

# Traffic

Traffic log messages record requests that a FortiWeb policy accepted or blocked. If the request was successful, it also includes the reply. Each log message represents its whole HTTP transaction.

Traffic logs do **not** record non-HTTP/HTTPS traffic such as FTP. This type of traffic is forwarded to your web servers if you have enabled IP-layer forwarding.

Traffic log messages are described below. For descriptions of header fields not mentioned here, see [Header & body fields on page 5](#).

## Meaning

Traffic matching and complying with a policy passed through or by FortiWeb.

If there is an error in the message, however, and the request/response used HTTPS, FortiWeb could not scan it. Depending on the mode of operation, an attack could have bypassed FortiWeb.

## Solution

Response times can often be improved, for example, by regular expression tuning, offloading SSL/TLS from your back-end server to your FortiWeb (especially if the model supports hardware acceleration), and/or offloading compression. For performance tips, see the [FortiWeb Administration Guide](#).

If HTTPS traffic is not flowing as you expect or not being inspected, and you have recently enabled HTTPS, typically this is due to a misconfiguration. The error message in the `msg` field will indicate the appropriate solution:

- `No Server Certificate for SSL Connection` — FortiWeb does not have the server certificate, so it cannot decode the SSL traffic. To fix this, upload the web server's certificate to FortiWeb.
- `SSL Certificate Key Mismatch` — An X.509 server certificate was uploaded to FortiWeb, but its private key did not match the one used by this HTTPS session. To fix this, upload the back-end web server's current certificate.
- `Ephemeral keys cannot be decrypted` — Ephemeral Diffie-Hellman key exchange can't be inspected due to the property of perfect forward secrecy, which makes real-time HTTPS inspection impossible. To fix this, disable ephemeral Diffie-Hellman on the back-end web server, and select a different key exchange method.
- `Unsupported Cipher for SSL Connection` — Either message digest (MAC) authentication failed or the MAC did not exist, or the transaction used an unsupported cipher suite. To fix this, on the back-end web server, disable cipher suites that are not supported by FortiWeb.
- `Unmonitored SSL Connection` — The HTTPS session was initiated before FortiWeb was deployed or before the server policy was enabled, so FortiWeb could not listen for the key exchange, and therefore cannot decrypt subsequent requests/responses in this HTTPS session. To fix this, on the back-end web server, clear HTTPS sessions and force clients to renegotiate.

If your appliance was operating in reverse proxy or true transparent proxy mode, the traffic was blocked, and no attack could have passed through to your protected web servers. **No action is required except to make sure that you have uploaded to FortiWeb the correct certificate for all protected web servers.**

Otherwise, if your appliance was:

- operating in offline protection or transparent inspection mode **or**
- configured only to **monitor** traffic (e.g. **Monitor Mode** was enabled or the **Action** is **Alert**, not **Alert & Deny**)

**examine the web server to determine whether or not an encrypted attack has passed through. You should also examine your web server's HTTPS configuration and disable cipher suites and key exchanges that are not supported by FortiWeb** so that during negotiation with clients, your web server does not agree to use encryption that FortiWeb cannot scan for attacks.

By the nature of log-only actions, detected attack attempts are logged but **not** blocked. You may also want to determine if the attack is from a single source IP address or distributed: blacklisting an offending client may help you to efficiently prevent further attack attempts, improving performance, until you can take further action.

By the nature of the network topology for offline protection mode (which can potentially cause differences in speeds of the separate routing paths), and asynchronous inspection for transparent inspection mode, **blocking cannot be guaranteed and some key exchanges are not supported**. For details, see the [FortiWeb Administration Guide](#).



Field name	Description
<b>ID</b> (log_id)	300000000 All traffic log messages share the same ID (log_id=300000000). See <a href="#">Log ID numbers on page 15</a> .
<b>Sub Type</b> (subtype)	http All traffic log messages share the same subtype (subtype=http). See <a href="#">Subtypes on page 16</a> .
<b>Level</b> (pri)	notification See <a href="#">Priority level on page 16</a> .
<b>Message</b> (msg)	<p>If the HTTP request triggered the FortiWeb web caching feature, the message begins with [Replied by Cache].</p> <p>The HTTP/HTTPS request's:</p> <ul style="list-style-type: none"> <li>• method</li> <li>• IP layer source and destination address and port numbers (IPv6 addresses are surrounded by square brackets to better demarcate the port number, e.g. [2001:470:19:ad7:6::230]:443)</li> </ul> <p>such as:</p> <ul style="list-style-type: none"> <li>• HTTP <b>GET</b> request from 10.0.2.5:8239 to 10.0.2.1:443</li> <li>• HTTP <b>POST</b> request from 10.0.2.5:8100 to 10.0.2.1:80</li> </ul> <p>If the transaction used HTTPS, and there was an error when either decoding it or participating in the handshake, there may be an error message instead of the HTTP method, such as:</p> <p>HTTP request from 192.0.2.1:40170 to 10.0.2.1:443, <b>Ephemeral keys cannot be decrypted</b></p>
<b>Source Country</b> (srccountry)	The country that is the source of the traffic.
<b>HTTP Content Routing</b> (content_switch_name)	The name of the associated HTTP content routing policy.
<b>Server Pool Name</b> (server_pool_name)	The name of the server pool in the associated server policy.

## Examples

```
date=2014-06-26 time=00:43:37 log_id=30000000 msg_id=000001351251 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=traffic subtype="http" pri=notice proto=tcp service=http status=success reason=none policy=Auto-policy src=10.0.8.103 src_port=8142 dst=10.20.8.22 dst_port=80 http_request_time=0 http_response_time=0 http_request_bytes=444 http_response_bytes=401 http_method=get http_url="/" http_host="10.0.8.22" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; " http_retcode=200 msg="HTTP GET request from 10.0.8.103:8142 to 10.20.8.22:80" srccountry="Reserved" content_switch_name="testa" server_pool_name="Auto-ServerFarm"
```

```
date=2014-04-11 time=09:26:22 log_id=30000000 msg_id=000000000156 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=traffic subtype="http" pri=notification proto=tcp service=https status=success reason="none" policy="policy1" src=172.20.120.47 src_port=53817 dst=172.20.120.47 dst_port=80 http_request_time=18 http_response_time=1 http_request_bytes=464 http_response_bytes=3060 http_method=get http_url="/index" http_host="172.20.120.48" http_agent="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" http_retcode=200 msg="HTTPS GET request from 172.20.120.47:53817 to 172.20.120.47:80 " srccountry="United States" content_switch_name="testa" server_pool_name="Auto-ServerFarm"
```

```
date=2014-04-11 time=10:16:29 log_id=30000000 msg_id=000000000230 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=traffic subtype="http" pri=notification proto=tcp service=http status=success reason="none" policy="policy1" src=172.20.120.46 src_port=49234 dst=172.20.120.48 dst_port=80 http_request_time=0 http_response_time=0 http_request_bytes=257 http_response_bytes=0 http_method=get http_url="/admin" http_host="172.20.120.48" http_agent="Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)" http_retcode=500 msg="HTTP POST request from 172.20.120.46:49234 to 172.20.120.48:80 " srccountry="United States" content_switch_name="testa" server_pool_name="Auto-ServerFarm"
```



*High Performance Network Security*



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.